OFICINA DE CONTROL INTERNO

INFORME DE AUDITORÍA

TIPO DE INFORME

Preliminar [ ] Definitivo [X]

AUDITORIA AL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN COLCIENCIAS

AÑO	AUDITORÍA	PROCESO, PROCEDIMIENTO O ACTIVIDAD	ÁREA RESPONSABLE
2019	A10	SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	• OFICINA TIC • DIRECCION ADMINISTRATIVA Y FINANCIERA • SECRETARIA GENERAL • TALENTO HUMANO

PERIODO AUDITADO O EVALUADO	FECHA INFORME PRELIMINAR	FECHA INFORME DEFINITIVO
2018-2019	16/09/2019	25/09/2019

Informe elaborado por:

Javier Herrera

Auditor
Oficina de Control Interno

CONTENIDO

INTRODUCCIÓN 3

1. OBJETIVOS 4
2. ALCANCE 4
3. RIESGOS EVALUADOS 5
4 HALLAZGOS 7
5. RECOMENDACIONES 17

INTRODUCCION

Las actividades de Auditoria Interna al Modelo de Seguridad y Privacidad de la Información se desarrollan en el marco del Plan de Auditoria de la Oficina de Control Interno, el cual tiene como propósito evaluar el cumplimiento de los requisitos la Norma Internacional ISO/IEC 27001:2013 Seguridad de la Información, para verificar el cumplimiento de las disposiciones establecidas en el Modelo de Seguridad y Privacidad de Información y la Estrategia Gobierno digital implementadas en Colciencias y así, comprobar que las actividades de han desarrollado y se mantienen de manera eficaz, llevando controles adecuados teniendo en cuenta los riesgos identificados dentro de la entidad.

Al finalizar se habrán encontrado las desviaciones que es necesario corregir para lograr elevar el cumplimiento en las actividades desarrolladas y asi permitir que la Seguridad en la Información se desarrolle eficazmente en cumplimiento de las directrices dadas.

1. OBJETIVO

El objetivo propuesto para el desarrollo de la presente Auditoria apunta a:

Evaluar el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, verificando el cumplimiento de las disposiciones establecidas en el Modelo de Seguridad y Privacidad de Información y la Estrategia Gobierno Digital, comprobando que se mantienen de manera eficaz los controles.

2. ALCANCE

El Alcance de la Auditoria, cubre las disposiciones establecidas en la Norma ISO/IEC 27001:2013 y las actuaciones realizadas en el Proceso de Control Interno y los lineamientos señalados en la Política de Seguridad y privacidad de la información estandarizados en el Sistema de Gestión de la Calidad - GINA.

3. RIESGOS EVALUADOS

En el marco de los objetivos y el alcance establecido para esta Auditoria se evalúan los riesgos actuales establecidos en el Mapa de Riesgos vigente y los riesgos potenciales identificados, que pueden afectar los resultados institucionales.

Al respecto se encontró que actualmente existen cinco (5) riesgos identificados en el Proceso Gestión de la Información, los cuales se relacionan en la siguiente tabla:

PROCESO	RIESGOS ACTUALES DEL PROCEDIMIENTO
Gestión de la Información	R 01-2019 Acceso indebido a la plataforma tecnológica de la Entidad generando uso inadecuado de la información, causando pérdida de la información, daño en los sistemas y/o vulneración de los mismos.
	R 02-2019 Posibilidad de daños en los equipos del Datacenter generando perdida de la integridad de la información de Colciencias.
	R 03-2019 Indisponibilidad de los servicios web de la Entidad, generando perdida de la disponibilidad de la información y demoras en los procesos internos de Colciencias.
	R 04-2019 Indisponibilidad de los servicios de la entidad debido a daños provocados por mal funcionamiento o uso de los equipos tecnológicos de Colciencias.
	R 05-2019 Perdida de la continuidad de los servicios y/o procesos de la entidad debido a la ausencia de un BCP " Plan de Continuidad del Negocio".

Los riesgos identificados durante la auditoria se tomaron del Plan de tratamiento Riesgos de Seguridad Digital 2019, desarrollados por la Oficina de Tecnologías de la Información y Comunicaciones – TIC, en este ejercicio de auditoria se pudo evidenciar que los Líderes de Proceso siguen las indicaciones dadas por a Oficina TIC para el cumplimiento del desarrollo del MSPI.

Igualmente se identificó que los riesgos potenciales a los que se ve expuesta la Entidad en el desarrollo de las actividades relacionadas con la presente Auditoria y que no están contemplados en el Mapa de Riesgos vigente para la entidad son:

RIESGOS POTENCIALES IDENTIFICADOS
1. Riesgo de no cumplimiento con los requisitos de las Partes Interesadas Pertinentes.
2. Riesgo de incumplimiento de requisitos por desarrollo de actividades desde la Oficina TIC y no contar con la participación activa de los Líderes de Proceso.
3. Riesgo de Materialización de los riesgos establecidos en el Plan de tratamiento Riesgos de Seguridad Digital 2019 al no evaluar la eficacia de las acciones establecidas.
4. Riesgo de pérdidas en los controles establecidos en el Sistema de Gestión de Seguridad de la Información al no llevar planificación de cambios en las diferentes actividades establecidos en la Política de Seguridad y Privacidad de la Información G104M01 010319 V2 para la Entidad.
5. Riesgo de no logro de las actividades establecidas en el en el Sistema de Gestión de Seguridad de la Información por no obtener toma de conciencia en los funcionarios de la Entidad.
6. Riesgo de perdida de control en el MSPI al no ser revisada por los Líderes de Proceso.
7. Riesgo de perdida de control de usuarios al nombrar muchos grupos con el mismo nombre.
8. Riesgo de generación de eventos al permitir que los usuarios ingresen a herramientas de configuración del sistema como el CMD desde su puesto de trabajo.
9. Riesgo de materialización de ataques a la Confidencialidad, Integridad o Disponibilidad de la Información al no hacer seguimiento a las actividades no permitidas de los usuarios en el sistema.
10. Riesgo de bajo cumplimiento en el Sistema de Gestión de Seguridad de la Información y cobertura deficiente en Seguridad de la Información al no aprobar las Políticas requeridas en forma obligatoria.
11. Riesgo de materialización de problemas al interior de la Entidad al no hacer seguimiento a los riesgos relacionados con las contrataciones externas.
12. Riesgo de perdida de control por no actualización de los Requisitos Legales establecidos para el en el Sistema de Gestión de Seguridad de la Información.

4. HALLAZGOS

Hallazgo No.	Numeral	Evidencia de la Auditoria	Tipo de Hallazgo
01	4.4	El soporte brindado por la Oficina TIC permite aumentar la eficacia en las actividades de control implementadas en el en el Sistema de Gestión de Seguridad de la Información.	Fortaleza
02	5.3	La asignación de roles y responsabilidades en cumplimiento de las disposiciones planificadas, hace que el seguimiento para el cumplimento de las actividades de las personas se desarrolle en forma eficaz.	Fortaleza
03	6.1.2a 8.2	La metodología establecida para el control de riesgos permite mantener implementados controles adecuados para el MSPI.	Fortaleza
04	7.2	El seguimiento, acompañamiento y soporte del proceso de Recursos Humanos permite monitorear el desempeño de las personas y genera confianza que aporta a la mejora del Clima Organizacional.	Fortaleza
05	A5.1.1	La definición de políticas y controles en el MSPI, permite obtener resultados adecuados y cumplir con los requisitos de cumplimiento para Seguridad de la Información.	Fortaleza
06	A8.2.1	Las actividades de control de archivo se mantienen controladas en cumplimiento de la Ley General de Archivos.	Fortaleza
07	A12.1.4	Las actividades de desarrollo se mantienen controladas en desarrollo, prueba y producción, actividades que permiten controlar la materialización de riesgos.	Fortaleza
08	A15.1.3	Se mantienen controladas las relaciones con los proveedores externos, actividades que favorecen los buenos resultados del MSPI.	Fortaleza
09	A16.1.3	Los reportes atendidos por la Mesa de Servicio hacen que la trazabilidad sea adecuada para las actividades de control del MSPI.	Fortaleza
10	A18.1.2	La identificación y cumplimiento de requisitos legales hacen que se fortalezcan las actividades implementadas en el Sistema de Gestión de Seguridad de la Información.	Fortaleza
11	A18.2.3	Las actividades de seguimiento desarrolladas por la Oficina de Tecnologías de la Información y Comunicaciones - TIC en el Sistema de Gestión de Seguridad de la Información permite desarrollar actividades eficaces de control.	Fortaleza

Hallazgo No.	Numeral	Evidencia de la Auditoria	Tipo de Hallazgo
01	6.1.3e	Desarrollar el tratamiento de riesgos a través de la consolidación de una Declaración de Aplicabilidad que soporte lo establecido en la Matriz Plan de Tratamientos de Riesgos de Seguridad Digital G101PR01M03 V02 24012019, permitirá desarrollar mejores controles dentro del Sistema de Gestión de Seguridad de la Información.	Mejora

Hallazgo No.	Numeral	Evidencia de la Auditoria	Tipo de Hallazgo
01	4.2a	En la Oficina de Tecnologías de la Información y Comunicaciones TIC deberían establecer cuando van a identificar las Partes Interesadas que son Pertinentes para el SG-SI con el fin de dar cumplimiento a los requisitos establecidos para determinar las Partes Interesadas que son Pertinentes al Sistema de Gestión de la Seguridad de la Información y ampliar el contenido de la Caracterización del Proceso de Tecnología G104 040619 V4 donde han identificado las Partes Interesadas del Proceso del SGC.	Observación
02	5.1	Podrían presentarse incumplimientos de alto impacto al desarrollar el cumplimiento de las actividades de Liderazgo y Compromiso por la Oficina de Tecnologías de la Información y Comunicaciones – TIC y no evidenciarse participación de la Alta dirección.	Observación
03	6.1.1d-e	Se presentarían problemas en la gestión al no evaluar la eficacia de las acciones establecidas para tratar los riesgos y oportunidades relacionados con los Activos de Información (Información Documentada) y los Activos de TI (Físicos) dentro del SG-SI.	Observación
04	8.2	Se generarían perdidas de control y materialización de riesgos al no llevar Controles de Cambios cuando se proponen u ocurren cambios significativos en el SG-SI donde se describan los cambios que se podrían presentar en la Entidad por la implementación de los controles en SI o valoraciones de riesgos.	Observación
05	7.3	Se evidenciarían incumplimientos en las actividades que desarrollan los funcionarios al no lograr que tomen conciencia con el contenido de la política de SI, la contribución a la eficacia del SG-SI incluyendo los beneficios de la mejora del desempeño de SI y las implicaciones de la no conformidad con los requisitos del SG-SI.	Observación
06	10.2	La Alta Dirección debería mejorar continuamente la conveniencia, adecuación y eficacia del SG-SI con la ejecución de la Revisión por la Dirección, tomando como referencia los resultados obtenidos en la Planificación y Operación del SG-SI.	Observación
07	A9.2.2	Se materializarían errores en la Operación al continuar creando diferentes grupos con el mismo nombre para el control de usuarios y la asignación de tarjetas.	Observación
08	A9.2.5	Tendrían que desarrollarse restricciones al sistema de información para no permitir que los usuarios ejecuten herramientas administrativas como el CMD teniendo en cuenta la vulnerabilidad que se presenta al poner en funcionamiento este comando.	Observación
09	A12.4.1	Se debería establecer una frecuencia más alta en las revisiones que se hacen a los logs en los servidores de la Entidad con el fin de asegurar que se controla la materialización de eventos o incidentes en el SG-SI.	Observación
10	A13.2.1	Se presentarían errores en el Control Operacional al no contar con las Políticas y procedimientos de transferencia de información y Política de desarrollo seguro implementadas dentro del SG-SI.	Observación
11	A14.2.1	Se mostrarían errores dentro del SG-SI al no establecer controles para reducir riesgos asociados a modificaciones, alteraciones, cambios o	Observación

		accesos no autorizados en sistemas en producción, teniendo en cuenta que se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la Entidad.	
12	A14.2.7	Podrían generarse errores dentro del SG-SI al no hacer controlar los riesgos relacionados con el desarrollo contratado externamente ya que estas actividades se deben supervisar y ser objeto de seguimiento por parte de la Entidad.	Observación
13	A18.1.3	Se encontrarían incumplimientos en la ejecución de cumplimiento del Control Operacional al continuar con la identificación de requisitos legales obsoletos en los documentos del SG-SI como la GP1000:2009.	Observación

Hallazgo No.	Numeral	Evidencia de la Auditoria	Tipo de Hallazgo
01	4.1 Conocimiento de la organización y de su Contexto	Se encontró incumplimiento en el análisis de la Entidad y su contexto evidenciado en que no se encuentran identificadas las cuestiones externas e internas que son pertinentes para el propósito del SG-SI y que afectan la capacidad para lograr los resultados previstos.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **se acepta** retirar la No Conformidad considerando que las Debilidades y Amenazas se interpretan como Cuestiones Internas y Cuestiones Externas.		
02	4.2b Comprensión de las necesidades y expectativas de las Partes Interesadas	Se verificó incumplimiento en el análisis de la comprensión de las necesidades y expectativas de las Partes Interesadas al evidenciarse que no se han identificados los requisitos de las Partes Interesadas que son Pertinentes para el SG-SI.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad porque en el Contexto Estratégico Colciencias 2019 G101PR01AN01 V01 no hay evidencia de las necesidades y expectativas de las Partes Interesadas.		
03	4.3 Determinación del alcance del SG-SI	Se pudo encontrar que el Alcance establecido para el SG-SI se encuentra mal elaborado al evidenciar que no se ha considerado los análisis del Conocimiento de la Organización y su Contexto, las Partes Interesadas que son Pertinentes y las interfaces y dependencias entre las actividades realizadas por la Entidad y las que realizan otras Organizaciones.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se han considerado las Partes Interesadas que son Pertinentes, así como las interfaces, dependencias entre las actividades realizadas por la Entidad y las que realizan otras Organizaciones.		
04	6.1.1 Acciones para tratar riesgos y oportunidades	Se halló que la planificación del SG-SI no se ha desarrollado en forma adecuada evidenciado en que no se consideraron las cuestiones referidas en el Conocimiento de la Organización y su Contexto y los requisitos referidos en la Comprensión de las necesidades y expectativas de las Partes Interesadas para determinar los riesgos y oportunidades que es necesario tratar dentro del SG-SI	No Conformidad

	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se han considerado los requisitos referidos en la Comprensión de las necesidades y expectativas de las Partes Interesadas para determinar los riesgos y oportunidades que es necesario tratar dentro del SG-SI		
05	6.1.1 a) Acciones para tratar riesgos y oportunidades	Al revisar las acciones para tratar riesgos y oportunidades no se pudo evidenciar que en el SG-SI se aseguren de que puedan lograr sus resultados previstos ya que estos no se encuentran identificados.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se han identificado los resultados previstos del SG-SI.		
06	6.1.1b-c Acciones para tratar riesgos y oportunidades	Al examinar las acciones para tratar riesgos y oportunidades no se pudo evidenciar que en el SG-SI se aseguren de que puedan prevenir o reducir efectos indeseados y logren obtener la mejora continua.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que al no contar con riesgos relacionados con los requisitos de las Partes Interesadas Pertinentes no se aseguran de que puedan prevenir o reducir efectos indeseados y logren obtener la mejora continua.		
07	6.1.2 c) 1 Valoración de riesgos de la seguridad de la información	En Regalías al en revisión de los controles para TIC se encontró que no se han valorado los riesgos de SI, se pudo evidenciar que no se ha aplicado un proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de la Confidencialidad, de la Integridad y de la Disponibilidad.	No Conformidad
08	6.1.3c Tratamiento de riesgos de la seguridad de la información	En los planes de acción establecidos en el documento Controles 27001_Plan de Trabajo, se encontró que no se han determinado las fechas de seguimiento a las actividades proyectadas, lo que permite evidenciar que no ha establecido el momento en el cual se llevara a cabo el comparativo de los controles actuales con los controles del Anexo A de la ISO/IEC 17001:2013.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se han determinado las fechas de seguimiento a las actividades proyectadas dentro de los planes de acción establecidos en el documento Controles 27001_Plan de Trabajo.		
09	6.1.3d Tratamiento de riesgos de la seguridad de la información	Analizando el tratamiento de riesgos de la seguridad de la información se pudo evidenciar que no se ha producido la Declaración de Aplicabilidad que contenga los controles necesarios con la justificación de las inclusiones y las exclusiones del Anexo A.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que en el SG-SI no se ha producido la Declaración de Aplicabilidad.		
10	6.1.3f Tratamiento de riesgos de la seguridad de la información	Durante el análisis del tratamiento de riesgos de la seguridad de la información no se pudo evidenciar que se haya obtenido por parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la SI.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se ha obtenido la aprobación del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la SI por parte de los dueños de los riesgos.		

11	7.4 Comunicación	En el desarrollo de la auditoria al indagar con los Lideres de Proceso de la Entidad se pudo evidenciar que no se ha determinado la necesidad de comunicaciones internas y externas pertinentes al SG-SI que incluyan el contenido de la comunicación, cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos para llevar a cabo la comunicación.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que para las comunicaciones internas y externas pertinentes al SG-SI no se han incluido los controles de cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos para llevar a cabo la comunicación.		
12	7.5.3 Control de la información documentada	En análisis de los controles establecidos se pudo evidenciar que para el manejo de la Información Documentada no se mantienen controles adecuados de archivo de información, se pudo evidenciar que los funcionarios consultan el correo electrónico para validar la información actualizada en lugar de consultar las carpetas establecidas para al almacenamiento de información.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que en la Auditoria se evidencio que para el manejo de la información se consultan los correos electrónicos y no las bases oficiales como Waira.		
13	9.1 Seguimiento, medición, análisis y evaluación	Al revisar el Indicador de Gestión Atención Incidentes de Seguridad implementado con una meta del 90%, se encontró que la última medición se desarrolló en el mes de Enero de 2019 con un resultados el 90%, se evidenció que durante el año 2019 no se ha vuelto a medir el Indicador teniendo en cuenta la frecuencia mensual establecida.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que el Indicador de Gestión Atención Incidentes de Seguridad fue implementado con una meta del 90% y frecuencia trimestral, en la Auditoria Interna se evidenció que la última medición fue desarrollada en el mes de Enero de 2019 y no se cuenta con seguimientos en las fechas establecidas.		
14	9.2 Auditoria Interna	Se encontró incumplimiento a las actividades de Auditoria Interna establecidas en el Procedimiento de Auditoria Interna E101PR03 V07 publicado en Gina, donde se encuentra establecido que la Auditoria Interna se debe desarrollar con frecuencia anual, se pudo evidenciar que la última Auditoria Interna al SG-SI se ejecutó en el año 2016.	No Conformidad
15	9.3 Revisión por la Dirección	En revisión de las actividades de cumplimiento de la Revisión por la Dirección no se encontraron desarrolladas, se pudo evidenciar que esta reunión se establece con una frecuencia anual y no se ejecutado en procura de verificar la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que la Revisión por la Dirección para el SG-Sino se ha desarrollado.		
16	A5.1.2 Revisión de las politicas para la seguridad de la información	Se halló que la actividad de revisión de la Politica de Seguridad y Privacidad de la Información G104M01 010319 V2 no se encuentra establecida en intervalos planificados o si ocurren cambios significativos, evidenciando que no se han asegurado de lograr su conveniencia, adecuación y eficacia continuas dentro del SG-SI.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que la Política de Seguridad y Privacidad de la Información G104M01 no se ha revisado en intervalos planificados para asegurar que se logra su conveniencia, adecuación y eficacia continua dentro del SG-SI.		

17	A6.2.2 Teletrabajo	Se pudo encontrar que no se ha implementado la política y las medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo ya que las actividades de Teletrabajo no se desarrollan en la Entidad, no se evidencia el desarrollo de la justificación de la no aplicabilidad de este Control.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que se hace referencia a la inexistencia de una Política de Teletrabajo, en el Control A6.2.2 de la Guía No. 8 Controles de Seguridad y Privacidad de la Información, se establece la implementación de una Política de Teletrabajo con las medidas adecuadas de seguridad y soporte para proteger la información de la Entidad a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo; en la auditoria se evidenció el desarrollo de las pruebas piloto, sin embargo dentro de la Política de Seguridad y Privacidad de la Información G104M01 010319 V2, no se encuentra el establecimiento de esta Política para su cumplimiento.		
18	A8.1.1 Inventario de activos	En Regalías en revisión de los controles para TIC se encontró que no se han identificado los activos asociados con información e instalaciones de procesamiento de información, se pudo evidenciar que no se ha elaborado ni mantenido un inventario de estos activos.	No Conformidad
19	A8.2.1 Clasificación de la información	Se verificó que en las actividades de gestión de correspondencia se recibe la documentación y se pasa a medio digital de acuerdo a los controles establecidos, se pudo evidenciar que en esta actividad no se verifica la cantidad de folios que ingresan a la Entidad.	No Conformidad
20	A8.3.3 Transferencia de medios físicos	Se encontró que los medios que contienen información son protegidos contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte, actividades establecidas en la Política de Seguridad y Privacidad de la Información G104M01 010319 V2 - 1.1.11 Política de Gestión de medios de almacenamiento / Transferencia de medios, se revisa el portátil HP S/N 5CG7452KDX, Placa 16700201516 encontrando ultima salida el 160819 e ingreso el 20081, controles establecidos Orden de Salida A103PR02F03 V03 21022019 y Control y registro de ingreso y salida de Portátiles fecha 010819, no se pudo evidenciar que la información almacenada en este Portátil cuente con controles de Criptografía.	No Conformidad
21	A9.2 Gestión de acceso de usuarios	Durante la auditoria realizada a los Archivos físicos se verificó que el acceso de los usuarios no se controla en forma adecuada, no se aplica el acceso no autorizado a los servicios de información, en el archivo de Gestión Humana se evidenció la entrada y salida de diferentes usuarios sin autorización formal y la asignación y custodia del archivo a la Sra. Luz Ángela Monroy Contratista sin autorización documentada, este manejo se desarrollo de forma verbal, en Regalías todos los usuarios tiene permisos de lectura, escritura y borrado, todos modifican la base principal en forma autónoma.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que se menciona el acceso no autorizado de los usuarios al archivo físico, en la auditoria desarrollada el 29 de Agosto de 2019 se evidenció autorización de custodia verbal dada al contratista asi como entrada y salida de diferentes funcionarios al archivo sin autorización formal, la Hoja de Control de Historia Laboral A101PR01F05 V02 17092019 no se presentó ni se utilizo durante el ingreso al archivo en el desarrollo de la Auditoria.		

22	A9.2.1 Registro y cancelación del registro de usuarios	En Regalías en revisión de los controles para TIC no se encontró la aplicación del registro y cancelación del registro de usuarios, se pudo evidenciar que se mantiene un Controlador de Dominio Server 2012R2 no configurado como Controlador de Dominio donde los usuarios no son controlados.	No Conformidad
23	A9.2.4 Gestión de información de autenticación secreta de usuarios	Durante la auditoria se pudo evidenciar que el Contratista OTIC dejo pegada su clave de acceso al aplicativo de asignación de permisos de dispositivos móviles generando incumplimiento a los controles establecidos en SI.	No Conformidad
24	A9.4.2 Procedimiento de ingreso seguro	Se halló el ingreso de comidas y bebidas a la zona segura de IT, en la Politica de Seguridad y Privacidad de la Información G104M01 010319 V2 en los controles de acceso físico se establece que en las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber, evidenciando incumplimiento a los controles establecidos para el SG-SI.	No Conformidad
25	A10.1.1 Política sobre el uso de controles criptográficos	Se encuentra desarrollado para el usuario Sonia Esperanza Monroy Subdirectora de la Entidad la firma del Acuerdo sobre uso del mecanismo de firma digital G104M01F02 V0 19032019, se puo evidenciar que el documento firmado se encuentra desarrollado el 12042019 - No cumple con control documental establecido por la Entidad.	No Conformidad
26	A10.1.1 Política sobre el uso de controles criptográficos	Se observó que las claves de acceso a las aplicaciones se mantienen listadas en un archivo Word el cual se encuentra protegido mediante números, letra y símbolos, se verifica acceso ok, se pudo evidenciar que estas claves son compartidas mediante WhatsApp, Hangouts y papeles escritos del usuario Iprojas sin control, actividad que pone en riesgo las actividades ya que las claves pierden control y se aumentan riesgos.	No Conformidad
27	A10.1.2 Gestión de llaves	En la revisión se validó incumplimiento a los requisitos del SG- SI, se pudo evidenciar que no se ha desarrollado ni implementado la política para el uso, protección y tiempo de vida de las llaves criptográficas durante el ciclo de vida.	No Conformidad
28	A11.1.2 Controles de acceso físicos	Durante la auditoria se pudo verificar bajo control en las actividades de seguridad en cuanto a control de acceso físico, se evidenció que las puertas del cuarto eléctrico y de rack del cuarto y quinto piso fueron abiertas con la tarjeta de visitante del Auditor.	No Conformidad
29	A11.1.3 Seguridad de oficinas, recintos e instalaciones	Se pudo hallar mala aplicación del control de Seguridad de oficinas, recintos e instalaciones, evidenciado en el proceso de cierre del dia 29/08/2019 en horario 7:00pm en los pisos 5 y 3 en donde la verificación de puertas cerradas de acuerdo al protocolo establecido por el personal de seguridad no se desarrolló.	No Conformidad
30	A11.1.4 Protección contra amenazas externas y ambientales	No se vio cumplimiento a los requisitos del SG-SI evidenciado en que no se ha diseñado y aplicado protección física contra desastres naturales para el cuidado de los archivos y la protección de activos físicos.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se hace referencia al no establecimiento de condiciones adecuadas para la conservación de la documentación, en la auditoria desarrollada el 03 de Septiembre de 2019 se evidenció que		

	no se cuenta con protección física contra desastres naturales (Inundación, terremoto, derrumbe o deslizamiento, entre otros), de acuerdo al Control A11.1.4 de la Guia No. 8 Controles de Seguridad y Privacidad de la Información donde se debe diseñar y aplicar protección física contra desastres naturales.		
31	A11.2.3 Seguridad del cableado	En la auditoria no se hallaron marquillas en los puntos de conexión del rack de comunicaciones ni las certificaciones de estos puntos de cableado estructurado con Fluke, no se pudo evidenciar con pruebas de funcionamiento la conectividad entre los puntos de las oficinas y los puntos del rack.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se hallaron marquillas en el cableado y los puntos del rack, ni las certificaciones de los puntos de red de datos.		
32	A11.2.4 Mantenimiento de equipos	Se validó que los equipos se mantienen correctamente para asegurar su disponibilidad e integridad continuas, al indagar por controles específicos no se pudo evidenciar los mantenimientos desarrollados a los aires acondicionados marca Emerson Serial 0011 Placa 0024 y Serial 0010 Placa 0025 ni a la UPS de 30kva del Data Center.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se pudieron evidenciar los mantenimientos desarrollados a los aires acondicionados y a la UPS del Data Center de la Entidad.		
33	A11.2.7 Disposición segura o reutilización de equipos	Se analizan los informes de los equipos destinados a dar de baja, encontrando estos con VoBo de IT desarrollados conforme a la resolución 1100 08082019, se evidenció que no se puede trazar ni garantizar que la información de estos equipos fue borrada en su totalidad pues no hay controles establecidos para esta actividad y no se mantiene control sobre el licenciamiento de los equipos para dar de baja ya que en el Anexo de la ficha técnica del comité de inventarios y baja de bienes (A103PR02F06 V01 121012917) fechado el 22112019 no se relacionan seriales del licenciamiento de estos equipos.	No Conformidad
34	A11.2.8 Equipos de usuario desatendido	Se halló en recorrido de las áreas de trabajo de la Entidad incumplimiento al control de equipos de usuario desatendido al evidenciar que los usuarios Marlen Pineda - Contratista, Edison Suárez - Gestor, Alejandra Gómez - Contratista y Andrea Castillo - Contratista dejaron sus Unidades Desatendidas.	No Conformidad
35	A11.2.9 Política de escritorio limpio y pantalla limpia	Se encontró en recorrido de las áreas de trabajo de la Entidad incumplimiento a la Política de escritorio limpio y pantalla limpia al evidenciar que los usuarios Paola Joya - Contratista, Jessica Vuelvas - Contratista, Liliana Rivera - Prof. Esp. y Leslie Silva - Contratista no cumplen con la Política de Escritorio despejado y pantalla despejada.	No Conformidad
36	A12.1.2 Gestión de cambios	No se vieron actividades de Gestión del Cambio desarrolladas en forma adecuada, se pudo evidenciar que en los cambios desarrollados a la Matriz de control de Activos donde pasan de controlar Activos de Información en las actividades del Proyecto IPv6 a controlar los Activos físicos y de Información de la Entidad y el control de inventarios de activos físicos de IT en la Entidad no se lleva planificación a los cambios.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que no se pudo evidenciar la Planificación del Cambio desarrollada para la Matriz de control de Activos donde pasan de controlar Activos de Información en el Proyecto IPv6 a controlar los Activos		

	físicos de la Entidad y el Control de Inventarios de activos físicos de la Entidad desde el retiro de Héctor Rodriguez a la actualidad.		
37	A12.3.1 Respaldo de la información	En Regalías en revisión de los controles para TIC se halló que generan copia incremental de la base principal (tamaño: 46.656k), se pudo evidenciar alta vulnerabilidad no controlada ya que esta copia se mantiene en almacenamiento local sin copia en medios removibles.	No Conformidad
38	A12.4.3 Registros del administrador y del operador	Se verifica que las actividades del administrador y del operador del sistema no se registran y no revisan con regularidad, se evidencia que estos registros no se tienen controlados, dentro de las Actas de Reunión de IT no se hace seguimiento a estos temas.	No Conformidad
39	A12.7.1 Controles de auditorias de sistemas de información	Se halla que los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se han planificado y acordado cuidadosamente para minimizar las interrupciones en los procesos del negocio, se pudo evidenciar que no se realizan auditorias desde el año 2016 al SG-SI.	No Conformidad
40	A13.2.2 Acuerdos sobre transferencia de información	Se analiza que los acuerdos para tratar la transferencia segura de información del negocio entre la organización y las partes externas no se ha aprobado, se pudo evidenciar que se mantiene en desarrollo la nueva versión de la Política de Seguridad y Privacidad de la Información G104M01 010319 donde esta política es incluida sin establecimiento de fecha de publicación, actividad que genera incumplimientos en el control del SG-SI.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que los acuerdos para tratar la transferencia segura de información del negocio entre la organización y las partes externas no se han aprobado.		
41	A15.2.1 Seguimiento y revisión de los servicios de los proveedores	Se hace revisión al contrato de Controles Empresariales firmado en 29062018 con objeto de renovación y adquisición de licencias configuración y parametrización de los productos y soporte técnico proactivo y reactivo de productos Microsoft, en las actividades establecidas para la revisión no se evidencia el desarrollo de las siguientes actividades: descripción de las actividades desarrolladas, descripción de las observaciones del supervisor, la descripción y la vida útil en las condiciones para reconocer como activo intangible.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que en las actividades establecidas para la revisión no se evidencia el desarrollo de las siguientes actividades: descripción de las actividades desarrolladas, descripción de las observaciones del supervisor, la descripción y la vida útil en las condiciones para reconocer como activo intangible.		
42	A15.2.2 Gestión de cambios en los servicios de los proveedores	Se halla seguimiento a las actividades de adición del contrato 335 de 2019, evidenciando que los riesgos relacionados con el manejo de la información y los controles de seguridad que se derivan del seguimiento de este riesgo no se mantienen controlados.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **se acepta** retirar la No Conformidad considerando que los riesgos relacionados con el manejo de la información fueron considerados.		

43	A16.1.5 Respuesta a incidentes de seguridad de la información	Se encontró que se establece la realización de sensibilización a todos los usuarios sobre incidentes de seguridad de la información, en estas actividades no se evidenció la mención a la respuesta que se debe dar a los incidentes en Seguridad de la Información.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **no se acepta** retirar la No Conformidad teniendo en cuenta que en la realización de sensibilización a todos los usuarios sobre incidentes de seguridad de la información no se menciona la respuesta que se debe dar a los incidentes en SI.		
44	A16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Se pudo verificar el conocimiento adquirido para analizar y resolver incidentes de seguridad de la información al presentarse la posibilidad de impacto o incidentes futuros, no se pudo evidenciar en el informe definitivo de auditoria de calidad E101PR03F10 V01 24102018 el desarrollo de Lecciones aprendidas para el tratamiento de las observaciones encontradas.	No Conformidad
45	A17.1.1 Planificación de la continuidad de la seguridad de la información	En la Entidad se han determinado los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, para una crisis o desastre se encuentra la Política de Seguridad y Privacidad de la Información G104M01 010319 V2 / 1.1.23. Política de Gestión de la Continuidad del Negocio, donde se establece que la Entidad cuenta con un Plan de Recuperación de Desastres que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, al verificar estas operaciones se pudo evidenciar que no hay resultados que permitan verificar el desarrollo de los planes de continuidad de negocios dentro del SG-SI.	No Conformidad
46	A17.1.2 Implementación de la continuidad de la seguridad de la información	Se analizó que en la Entidad se han establecido e implementado controles para asegurar el nivel de continuidad de negocio requerido para la SI durante una situación adversa, se evidencia el Plan Estratégico de las TIC 2019 - 2022 G101PR01N04 V01 31012019 a ejecutar dentro de este cuatrienio, se pudo evidenciar que las actividades de seguimiento a este Plan de Continuidad no se han desarrollado.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **se acepta** retirar la No Conformidad considerando que Plan Estratégico de las TIC 2019 - 2022 se encuentra desarrollado y puesto para ejecución.		
47	A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Se pudo encontrar que en la Entidad se han implementado controles a intervalos regulares para la continuidad de la SI con el fin de asegurar que son válidos y eficaces durante situaciones adversas, se pudo evidenciar que se proyecta la ejecución de actividades sin resultados dentro del SG-SI.	No Conformidad
	Según la observación presentada en el Memorando 20196300329443 del 23092019 **se acepta** retirar la No Conformidad considerando que se proyecta la ejecución de actividades con los resultados dentro del SG-SI.		

48	A18.2.1 Revisión independiente de la seguridad de la información	Se halla que el enfoque de la Entidad para la gestión de la seguridad de la información y su implementación no se revisan independientemente a intervalos planificados o en los cambios significativos, se evidencia el monitoreo desarrollado por Oficina de Tecnologías de la Información y Comunicaciones - TIC, pero no de cada oficina en forma independiente en términos de Seguridad de la Información.	No Conformidad
49	A18.2.2 Cumplimiento con las políticas y normas de seguridad	No se encontró cumplimiento con las políticas y normas de seguridad, se pudo evidenciar que los Líderes de Proceso no revisan con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su proceso como actividad de responsabilidad, con las políticas y normas de seguridad apropiadas y requisitos de seguridad.	No Conformidad

5. RECOMENDACIONES

El Plan de tratamiento de los riesgos se ha establecido conforme a lo establecido en la Matriz Plan de Tratamientos de Riesgos de Seguridad Digital G101PR01M03 V02 24012019, desarrollar este tratamiento conforme a lo encontrado en la Declaración de Aplicabilidad, permitiría desarrollar mejores controles dentro del MSPI.

6. PLAN DE MEJORAMIENTO

Con base en este informe definitivo, se solicita a la Oficina TIC, Secretaria General (Talento Humano) y la Dirección Administrativa y Financiera como dependencias responsables, se elabore un Plan de Mejoramiento, en el formato adjunto, que dé solución a los hallazgos identificadas y sea remitido a la Oficina de Control Interno para su aprobación, dentro de los ocho (8) días hábiles siguientes al recibo del presente informe.

Se recuerda que las acciones del Plan de Mejoramiento deben ser preventivas y/o correctivas, según el caso y requieren ser formuladas de manera efectiva para subsanar las debilidades encontradas, cuyas actividades no deben ser superiores a un año a partir de la suscripción del Plan en la Oficina de Control Interno.

Igualmente es necesario tener en cuenta que si en la ejecución de las acciones de mejora que se propongan se requiere la participación y responsabilidad de otras dependencias, la dependencia responsable del proceso auditado deberá coordinar con dichas dependencias la elaboración del Plan de Mejoramiento, antes de la presentación del Plan a la OCI.

JAVIER HERRERA - AUDITOR SEGURIDAD DE LA INFORMACIÓN

GUILLERMO ALBA CARDENAS – JEFE DE OFICINA DE CONTROL INTERNO