FECHA DEL INFORME:	30/09/2019	**PROCESO AUDITADO:**	Gestión de Riesgo Operativo
LIDER DEL PROCESO:	Jefe Oficina de Riesgos	**AUDITADOS:**	Claudia Stella Cortés – Coordinadora de Riesgos No Financieros Invitadas: Andrea Victoria Queruz – Oficina de Relaciones Internacionales Luz Marina Carreño – Vicepresidencia de Fondos en Administración
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Principal Oficina de Riesgos Piso 3 04/09/2019 – 05/09/2019	**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 Riesgo Operativo, 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 y la disponibilidad de la información. Igualmente, se destaca como fortaleza el liderazgo del SGSI y MSPI desde la Oficina de Riesgos, para la implementación, mantenimiento y mejora de los mismos, con la coordinación de acciones en toda la entidad.

4. RESULTADOS

CRITERIO DE AUDITORIA	NO CONFORMIDAD	OPORTUNIDAD DE MEJORA
Norma ISO 27001:2013 4 Contexto de la Organización 4.1. Comprensión de la organización y su contexto MSPI (Modelo de		Se recomienda incluir como partes interesadas del SGSI otro tipo de colaboradores, además de los funcionarios (contratistas, temporales, personal de proveedores trabajando in-house), no sólo desde su rol de “proveedores”, para mejorar el entendimiento de las

Seguridad y Privacidad de la Información).Fase de planificación Contexto de la entidad		expectativas de las partes interesadas.
Norma ISO 27001:2013 4 Contexto de la Organización 4.3.Determinación del alcance del SGSI		Se recomienda basarse en la Norma ISO 27003, la cual contiene una Guía de implementación de un SGSI. En esta norma, en lo aplicable a “Alcance” recomienda establecer límites físicos, procesos de la organización y activos de información cubiertos (incluyendo los activos de TIC:Hw, Sw, BDs).
MSPI (Modelo de Seguridad y Privacidad de la Información).Fase de planificación Política de Seguridad y Privacidad de la Información		Se recomienda definir objetivos específicos para el Sistema de Gestión de Seguridad de la Información, a partir de los lineamientos de la política; estableciendo y/o relacionando los planes para conseguirlos (actividades, recursos específicos, responsable con nombre y cargo, fecha de finalización, entregables, indicadores o forma de evaluar los resultados).
Norma ISO 27001:2013 Anexo A Dominio A.8 Gestión de activos A.8.2. Clasificación de la información Ley 1712 de 2014		En la “Guía para la clasificación de activos de información” - G176 no es clara la valoración de los diferentes tipos de activos (como instalaciones o infraestructura, hardware y roles críticos). En el mismo documento, sección de “Metodología de clasificación de activos de información” se indica que los activos que contengan datos personales obtienen una calificación de 60 en confidencialidad, lo cual corresponde a “información reservada”. Esto no concuerda con la Ley 1712 de 2014.
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.		Se requiere actualizar el inventario de activos de información, teniendo en cuenta los siguientes aspectos observados: • No están claros los tipos de activos, con qué criterio se clasifican y qué activos puede incluir cada categoría. (Ej. En tipo “servicio” se mezclan aplicativos, manual de procesos, proveedor de precios de valoración, aplicativo Avamar, etc). • Se incluyen en el inventario como un solo activo, todas las BD de los sistemas de información, impidiendo su calificación, identificación y valoración individual. • No se encuentran incluidos en el inventario todos los sistemas de información y aplicativos (tipo software), todos los servidores, equipos de comunicaciones, etc (tipo hardware). Se

		recomienda integrar o complementar el inventario con la información de la CMDB que administra la Dirección de Tecnología. • Las ubicaciones de los activos son muy generales. Se recomienda incluir el nombre del equipo o la carpeta compartida específicos, para los activos digitales.
Decreto 1080 de 2015		Los instrumentos de gestión de información pública (registro de activos de información e índice de información clasificada y reservada) deben ser adoptados y actualizados por acto administrativo, en cumplimiento del Decreto 1080 de 2015 (artículo 2.8.5.2.). El acto administrativo definido por la entidad para tal fin, debe estar correctamente conformado y conservar la evidencia.
Norma ISO 27001:2013 Anexo A A.6.1.5. Seguridad de la información en proyectos		Se recomienda documentar y formalizar la implementación de la matriz de contratos para la identificación, valoración y tratamiento de riesgos de proyectos de la entidad.
Norma ISO 27001:2013 9.1. Seguimiento, medición, análisis y evaluación	Se presenta incumplimiento de los requisitos de la Norma Técnica ISO 27001:2013, numeral 9.1. Seguimiento, medición, análisis y evaluación, dadas las siguientes situaciones: • Se presentó incumplimiento con la meta del indicador “Gestión de vulnerabilidades de la plataforma tecnológica”, para el primer semestre de 2019, obteniendo un resultado del 10%, siendo la meta alcanzar un 85% de remediación de vulnerabilidades críticas y altas detectadas. No se evidencia la documentación de un plan de mejoramiento frente a esta no conformidad, en el Formato F181. • Los indicadores de gestión de Seguridad y Privacidad de la Información no se encuentran publicados en un documento con la descripción de los mismos; como lo exige el MSPI de MinTIC; a pesar de que se menciona dicho documento dentro del Modelo de Seguridad y Privacidad de la Información	

	de la entidad (M16-versión 2). • Los indicadores operativos presentados en la auditoría no se encuentran reflejados en la caracterización del proceso (Implementación del SGSI y Concienciación en seguridad digital).	
Norma ISO 27001:2013 Anexo A A.17. Aspectos de seguridad de la información para la gestión de continuidad de negocio		Se recomienda establecer, ejecutar y hacer seguimiento a un cronograma de pruebas para el plan de continuidad de negocio, de manera integral. Esto se debe hacer una vez se haya actualizado el plan, considerando los nuevos sistemas de información, el cambio del centro de cómputo, los movimientos de las dependencias entre sedes, etc. En dicha prueba se deben verificar y evaluar los controles establecidos para garantizar la seguridad de la información en situaciones adversas.
Modelo de Seguridad y Privacidad de la Información. Resultados de fase de Planificación, Implementación y Evaluación de Desempeño	Se presenta incumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información de MinTIC, en tanto no se cuenta con los siguientes documentos: • Documento con el plan de comunicación, sensibilización y capacitación en seguridad y privacidad, para la entidad. • Documento con la estrategia de planificación y control operacional, aprobado por la Alta Dirección. • Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	
Norma ISO 27001:2013 Anexo A A.16. Gestión de incidentes de seguridad de la información		Se debe mantener actualizado el registro de los planes de respuesta a los incidentes de seguridad de la información dentro del aplicativo Vigía, puede ser anexando el formato F393 diligenciado; con el fin de hacer seguimiento y conservar evidencias de las acciones correctivas implementadas para evitar que se vuelva a presentar.
Norma ISO 27001:2013 Anexo A A.16. Gestión de incidentes de seguridad		Se recomienda asegurar que se gestionan los eventos de materialización de riesgo operativo que se puedan considerar

de la información		igualmente incidentes de seguridad de la información, a través de los procedimientos definidos en ambos sistemas de gestión del riesgo.
Norma ISO 27001:2013 Anexo A A.6.1.4. Contacto con grupos de interés especial MIPG – II Política de Seguridad Digital - FURAG		Se recomienda establecer contacto para pertenecer al CSIRT de Gobierno, así como con el Comando Conjunto Cibernético de las Fuerzas Armadas (CCOC), con el fin de establecer sinergias para fortalecer la ciberseguridad de la entidad e implementar la identificación de las infraestructuras críticas cibernéticas de la entidad.
Norma ISO 27001:2013 Anexo A A.6.1.4. Contacto con grupos de interés especial MIPG – II Política de Seguridad Digital - FURAG		Se debe definir y oficializar el responsable de ejercer el rol del enlace de seguridad digital y comunicarlo a CSIRT Gobierno, Colcert, MinTIC, CCOC y Coordinación Nacional de Seguridad Digital de la Presidencia de la República.
Decreto 1008 de 2018 Manual de Implementación de la Políticas de Gobierno Digital		Es importante para la entidad contar con el rol de Oficial de Seguridad de la Información, el cual, de acuerdo con el Manual de Implementación de la Políticas de Gobierno Digital, debe pertenecer a la Alta Dirección, participar en los Comités Institucionales de Gestión y Desempeño, liderar la implementación del MSPI y ejecutar las acciones específicas sobre seguridad y privacidad de la información definidas en el Marco de Referencia de Arquitectura Empresarial del Estado.
Decreto 886 de 2014 Decreto 90 de 2018 Ley 1581 de 2012		Se recomienda que, para el Registro Nacional de Bases de Datos, se tome como insumo el inventario de activos de información; revisando y teniendo en cuenta los activos que tienen información clasificada; con fundamento legal en la Ley 1581 de 2012.
Ley 1581 de 2012 Decreto 886 de 2014 Decreto 90 de 2018		Se evidencia que se presenta una inconsistencia en el diligenciamiento de los datos del “encargado” de las Bases de datos personales registradas ante la SIC; porque se registraron los datos de la Coordinadora de Riesgo No Financiero en la mayor parte de los casos. Se recomienda revisar la definición de “encargado” de la Ley 1581 de 2012.
Ley 1581 de 2012		Para el otorgamiento de servicios de programas internacionales se recomienda

Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015)		priorizar y documentar las acciones que se están tomando para recoger y almacenar la autorización para el tratamiento de datos personales de los beneficiarios de las becas para colombianos, en el aplicativo SEPI; así como de los programas Beca Colombia, Expertos Internacionales y Jóvenes Talentos, en convenio con Colfuturo. En este último caso, se debe asegurar el almacenamiento y disponibilidad de consulta para ICETEX de la autorización para el tratamiento de datos personales; en cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013. Igualmente, es urgente su implementación porque a través del uso de la plataforma de Colfuturo, se asegurará un canal más seguro para la recepción de documentación que contiene datos personales de los extranjeros.
Ley 1581 de 2012 Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015) Circular 8 de 2017 - Superintendencia de Industria y Comercio		Se requiere validar jurídicamente las causales de excepción contenidas en el Artículo 26 de Título VIII de la Ley 1581 de 2012, referente a la Transferencia de datos a terceros países. En caso de determinar que no se cumpla con alguna de ellas, se debe garantizar contar con la autorización expresa del beneficiario de transferir sus datos personales a otros países y por otra parte, asegurar que dichos países se encuentran en la lista de países aprobados por la SIC (Ver Circular 8 de Diciembre de 2017). Adicionalmente, se deben implementar canales seguros para la trasferencia de dicha información.
Ley 1581 de 2012 Guía para la implementación del principio de responsabilidad demostrada - SIC		Se recomienda implementar una gestión específica para los riesgos asociados con el tratamiento de datos personales, la cual puede complementar la gestión actual de riesgos de seguridad digital con el fin de implementar el principio de responsabilidad demostrada (accountability).
Norma ISO 27001:2013 Anexo A A.18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales		Se recomienda revisar y actualizar el normograma del proceso de Gestión de Riesgo Operativo, incluyendo normas y decretos reglamentarios sobre seguridad, privacidad y protección de datos, como: Decreto 1080 de 2015 Decreto 886 de 2014 (compilado en el Decreto 1074 de 2015) Decreto 103 de 2015 Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015) Resolución 3564 de 2015

		Decreto 1377 de 2013 Capítulo III Políticas de tratamiento Decreto 90 de 2018
Decreto 1081 de 2015	Se presenta incumplimiento del Decreto 1081 de 2015, dadas las inconsistencias presentadas en la información diligenciada en los instrumentos de gestión de información pública: • No se evidencia un estándar claro para diligenciar los datos de: “Medio de conservación y/o soporte” y “Formato”. • En el campo “Información publicada o disponible” no se puede diligenciar como “no publicable”, dado que se trata de un activo que contiene información pública. • Los enlaces a las publicaciones no funcionan. En cuanto al índice de información clasificada y reservada, se debe revisar lo siguiente: • No hay un estándar para el diligenciamiento de “Medio de conservación y/o soporte”. Puede ser solamente físico-análogo o digital-electrónico. • El responsable de producción de la información puede ser una dependencia o entidad externa; pero hay algunos casos en que para el activo este campo se diligencia con “sistema”, por ejemplo. Igualmente, se evidenció en auditorías a otros procesos que no está correctamente diligenciado este campo. • El responsable de la información debe ser una dependencia encargada del control de la información; sin embargo, se diligenció con cargos específicos, no por áreas. • No se encuentran diligenciados los campos “Fundamente jurídico de la excepción”, “Excepción total o parcial” v	

	"Plazo de la clasificación o reserva"	

Ley 1581 de 2012 Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015)		Se recomienda revisar dentro de la política de protección de datos personales publicada, los siguientes aspectos: • No se evidencia la finalidad de atención de peticiones, quejas y reclamos. • No se evidencia la fecha de aprobación y publicación. • Hace referencia a un procedimiento para el tratamiento y protección de datos personales, que no se encuentra publicado en In-Process, como procedimiento sino como guía. • La versión publicada al inicio de esta auditoría incluía un formato de autorización de tratamiento de datos que no estaba aplicando.

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 3 "no conformidades" con respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Así mismo, quedan abiertas 2 no conformidades provenientes de la auditoría anterior. Todas las anteriores (5) deben ser corregidas y analizadas para definir e implementar acciones correctivas, de acuerdo con el procedimiento de la entidad.

Adicionalmente, se detectaron en la auditoría 20 oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro. Por otra parte, como resultado del seguimiento a los planes de mejoramiento de la auditoría interna anterior, realizada a finales de 2017; se cerraron 9 no conformidades, de las 11 que estaban pendientes, aunque se dejaron recomendaciones y observaciones para algunas de ellas (Ver F86 anexo).

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.