FORMATO INFORME

INFORME 16A
AUDITORIAS PRIMARIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE CAJA HONOR VIGENCIA 2019

PREPARADO POR:

LUIS CARLOS RIVERA TORRENEGRA
AUDITOR LÍDER ISO 27001:2013

JUNIO DE 2019

FORMATO INFORME

INFORME AUDITORIAS PRIMARIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE CAJA HONOR VIGENCIA 2019

PREPARADO POR:

LUIS CARLOS RIVERA TORRENEGRA
AUDITOR LÍDER ISO 27001:2013

JUNIO DE 2019

Auditoría:	AUDITORÍAS INTERNAS PRIMARIAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 2019
Fecha Auditoría:	13/May/2019
Fecha Informe:	06/Jun/2019
Objetivo:	Determinar la eficacia, eficiencia y efectividad del Sistema de Gestión de Seguridad de la Información de conformidad con los requisitos de la Norma ISO 27001:2013. Hacer seguimiento a los hallazgos detectados en la auditoria de certificación de ICONTEC, realizada en noviembre de 2018 y las auditorías internas primarias y secundarias de 2018, de conformidad con los criterios establecidos por la Norma ISO 27001:2013 y verificar su estado actual.
Alcance:	De acuerdo con las auditorías de certificación de la norma ISO 27001:2013 realizadas por ICONTEC en la vigencia 2018, se obtuvo la certificación para los procesos de Gestión Estratégica, Gestión de Tesorería, Gestión de Finanzas y Crédito, Servicios Administrativos y Gestión disciplinaria. Por lo anterior, la presente auditoria evaluó el estado actual del Sistema de Gestión de la Seguridad Información de conformidad con los requisitos de la Norma ISO 27001:2013 a los siguientes procesos ya certificados así: Gestión informática, Gestión del SAC, Administración de Cuentas, Gestión del Trámite, Gestión del Riesgo, Gestión Jurídica, Gestión de Contratación, Gestión del Talento Humano, Gestión Estratégica, Gestión de Tesorería, Gestión de Finanzas y Crédito, Servicios Administrativos, Gestión Disciplinaria Por otra parte, se informa que se realizó la validación de requisitos de la Norma ISO 27001:2013 para los siguientes procesos que se proyectan certificar por parte de ICONTEC en la vigencia 2019 así: Gestión de Vivienda y Mercadeo, Gestión de Comunicaciones, Gestión Documental, Auditoría y Control.
Descripción Auditoría:	Conforme al programa de Auditorías Internas, aprobado para la vigencia 2019, la OFCIN presentó el Cronograma de Auditorias Primarias del Sistema de Gestión de Seguridad de la Información de Caja Honor, que se llevó a cabo en sitio desde el 13 de mayo al 13 de junio de 2019.

EQUIPO AUDITOR

Nombre	Cargo	Auditores	Líder
Luis Carlos Rivera Torrenegra	Profesional Especializado	☐	☑
Jhon Jairo Rosas Alba	JEFE OFICINA ASESORA SECTOR DEFENSA	☑	☐
Lina María Rendón Lozano	JEFE OFICINA ASESORA DE PLANEACIÓN	☑	☐
María Del Pilar Otavo Serrano	Profesional Especializado	☑	☐
Martha Patricia Reyes Gómez	Profesional Especializado	☑	☐
Sandra Maritza García Espitia	Profesional Especializado	☑	☐
Magda Milena Galeano Coronado	Profesional Especializado	☑	☐
Carlos Arturo Contreras Meza	Profesional Especializado	☑	☐
Norma Astrid Vargas Panqueba	Profesional Especializado	☑	☐
Diana Milena Hernández Mendoza	Profesional Especializado	☑	☐
Raul Wexler Pulido Téllez	Contratista	☑	☐

PERSONAL ENTREVISTADO

Nombre	Cargo
Lina María Rendón Lozano	Jefe Oficina Asesora De Planeación
Jhon Jairo Rosas Alba	Jefe Oficina Asesora Sector Defensa
Martha Cecilia Mora Correa	Jefe De Oficina Sector Defensa
Diana María Ospina Herrera	Jefe Oficina Asesora Sector Defensa
Ricardo Ignacio Becerra Borras	Jefe Oficina Asesora Sector Defensa
Gustavo Vizcaya Villa	Jefe Área Técnica y de Promoción
Sandra Patricia Pachón Bernal	Profesional Especializado

Ana Ilde Olarte Estupiñan	Profesional Especializado
Sonia Janeth García Ávila	Profesional Especializado
Jorge Iván González Patiño	Profesional Especializado
Ana Milena Rosero Alvarez	Profesional Especializado
Sandra Maritza García Espitia	Profesional Especializado
Natalia Eugenia Casas Quibano	Profesional Especializado
Diana Milena Hernández Mendoza	Profesional Especializado
Sandra Milena Ulloa Calvo	Profesional Especializado
Gladys Rivera Espinosa	Profesional Sector Defensa
Janefriend Carolina Ducuara Granados	Profesional Sector Defensa

DOCUMENTACIÓN ANALIZADA

Informes de auditorías internas y externas, documentación (caracterización, procedimiento, manuales, formatos, entre otros.) de los procesos divulgados a través de herramienta Isolucion, Norma ISO/IEC 27001:2013, así como la normatividad interna y externa aplicable.

REPORTE DE NO CONFORMIDADES Y OBSERVACIONES

Proceso	# No Conformidades
GESTIÓN DEL RIESGO	Se evidenció durante la revisión de la matriz de activos de información que esta requiere ser validada y completada para los procesos acorde a los lineamientos del Manual de Seguridad de la Información y Ciberseguridad y de la guía de Gestión de Activos de Información, por lo anterior es pertinente dar cumplimiento a los controles A.8.2.1 Clasificación de la información y A.8.2.2 Etiquetado de la información de la norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	Durante la auditoría realizada al proceso de Gestión de Comunicaciones, la líder explica que realiza las solicitudes de permisos a través de la herramienta System Center Service Manager, sin embargo a través de correo electrónico informó que había dos funcionarios de su área que pueden instalar programas y solicitó que se retiraran esos permisos. En el ejercicio de validación se verificó que se hubieran retirado los permisos, encontrando que esos dos funcionarios podían descargar programas sin autorización, para la prueba se descargó Spotify en los equipos de los dos funcionarios aunque no permitía el uso de la aplicación, por lo cual es

	pertinente dar cumplimiento al control A.9.2.3 Gestión de derechos de acceso Privilegiado de la Norma ISO/IEC 27001:2013.
ADMINISTRACIÓN DE CUENTAS	Durante la prueba de recorrido del proceso de administración de cuentas, se identifica en el lugar de los papeles que son objeto de reciclaje, documentos los cuales contienen información de datos personales de afiliados, información de cuentas individuales y certificados de haberes, evidenciando un inadecuado manejo de los activos de información del proceso, lo anterior en cumplimiento con lo establecido en los numerales A.8.1 "Responsabilidad por los activos" y A.18.1.4 "Privacidad y protección de información de datos personales" de la Norma ISO/IEC 27001:2013.

ASPECTOS FAVORABLES

PROCESO	OBSERVACIÓN
PLANEAR	
ADMINISTRACIÓN DE CUENTAS	Se evidencia conocimiento de la política por parte de la líder del proceso de Operaciones y de los funcionarios en cumplimiento del control A.5.1.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE COMUNICACIONES	Se destaca que la líder del proceso cuenta con amplio conocimiento en las políticas contenidas en el Manual de Seguridad de la Información y Ciberseguridad, cumpliendo con el control A.5.1.1 Política para la seguridad de la información de la Norma ISO/IEC 27001:2013.
GESTIÓN DE FINANZAS Y CRÉDITO	Se evidencia conocimiento en la política de Seguridad de la Información y Ciberseguridad por parte de la líder del proceso y sus colaboradores cumpliendo con el control A.5.1.1 Política para la seguridad de la información de la Norma ISO/IEC 27001:2013.
GESTIÓN DE TESORERÍA	La líder demuestra conocimiento y aplicación de la política acorde a los pilares de confidencialidad, integridad y disponibilidad. Lo anterior en cumplimiento al numeral 5.1 literal a) y el control A.5.1.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE TESORERÍA	La líder del proceso manifiesta que desde la estructura organizacional y en cumplimiento de las disposiciones de la Superintendencia Financiera de Colombia, se establece la separación de los deberes y responsabilidades del Back, Front y Middle Office. Lo

	anterior en concordancia con el control A.6.1.1 de la Norma ISO/IEC 27001:2013
GESTIÓN DEL RIESGO	Se evidencia conocimiento del Líder del Proceso en la gestión de la herramienta 3PAR, relacionado con el monitoreo y lectura de las alertas, lo anterior en cumplimiento del Control A.17.2.1 Disponibilidad de instalaciones de procesamiento de información, de la Norma ISO/IEC 27001:2013.
GESTIÓN DEL SAC	Se evidencia conocimientos tanto de la líder del proceso como de sus colaboradores del sistema de seguridad de la información, toda vez que solicita información a los funcionarios y dan cumplimiento al Numeral A.5.1.1 Política para la seguridad de la información de la Norma ISO/IEC 27001:2013.
GESTIÓN DEL TALENTO HUMANO	El proceso de Gestión del Talento Humano, verifica los antecedentes de los candidatos y estudio de seguridad, tales como: fiscales, penales, entre otros. La líder del proceso auditado muestra evidencias del último ingreso, certificados de contraloría, procuraduría y de la policía nacional, dándole la importancia apropiada al proceso de selección de personal, acorde a lo establecido en el Control A.7.1.1 Selección de la Norma ISO/IEC 27001:2013.
GESTIÓN ESTRATÉGICA	El proceso de Gestión Estratégica, evidencia que cuenta con una Matriz de Riesgos de Seguridad de la Información y detalla como aplica la valoración de riesgos acorde al Numeral 6.1.2 Valoración de riesgos de la seguridad de la información de la Norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	El líder del Proceso de Gestión Informática explica la normatividad que le aplica al proceso y bajo la misma se realiza la planificación para asegurar su cumplimiento (Circulares 042/12, 007/18, 005/19), acorde al numeral 4.1 Conocimiento de la organización y de su contexto, de la Norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	El líder del Proceso de Gestión Informática explica los 3 pilares de la política de la seguridad de la información acorde al numeral 5.1 Liderazgo y compromiso de la Norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	En el Proceso de Gestión Informática se evidencian reuniones semanales, inducciones y capacitaciones, en cumplimiento al numeral 7.3 Toma de conciencia de la Norma ISO/IEC 27001:2013.

HACER	
ADMINISTRACIÓN DE CUENTAS	Se evidencia el cumplimiento del numeral A.6.2.1 de la Norma ISO/IEC 27001:2013, a través del conocimiento y control en el cumplimiento de la política para dispositivos móviles, mediante formato de seguimiento a los funcionarios frente al uso de dispositivos móviles y verificación constante de su aplicabilidad.
GESTIÓN DE TESORERÍA	La líder del proceso de Gestión de Tesorería, manifiesta que los procesos de Gestión del Riesgo y Gestión Disciplinaria, son los responsables de emprender acciones para los usuarios que hayan infringido las políticas de seguridad de la información y ciberseguridad de Caja Honor, demostrando un amplio conocimiento en las gestiones a realizar, lo anterior en concordación con el A.7.2.3 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE VIVIENDA Y MERCADEO	El proceso de Gestión de Vivienda y Mercadeo, evidencia listas de asistencia de capacitación de seguridad de la información por parte del jefe del proceso a los funcionarios, dando cumplimiento al Control A.5.1.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN JURÍDICA	El proceso de Gestión Jurídica presenta una muy buena toma de conciencia y aplicación de los controles y el conjunto de políticas de seguridad de la información, dando cumplimiento al Control A.5.1.1 de la Norma ISO/IEC 27001:2013.
VERIFICAR	
GESTIÓN DE TESORERÍA	En las pruebas aleatorias practicadas, se evidencia el cumplimiento de la política de escritorio limpio Lo anterior en cumplimiento del Control A.11.2.9 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	Se evidencia durante el desarrollo de la auditoría que se encuentra implementada la política de seguridad de la información en los contratos con los proveedores dando cumplimiento al Control A.15.1 Seguridad de la información en las relaciones con los proveedores, de la Norma ISO/IEC 27001:2013.

ACTUAR	
GESTIÓN DOCUMENTAL	El proceso de Gestión Documental, realiza una excelente labor frente al seguimiento del proveedor de servicios de custodia de documentos teniendo en cuenta que realiza seguimiento trimestral al proveedor mediante un formato en Calidad identificado como GD-NA-FM 009 FORMATO DE VISITA BODEGAJE ARCHIVO CENTRAL, en la cual se incluyen temas relacionados a la gestión de la preservación y seguridad de los documentos en custodia y se hace seguimiento a las condiciones ambientales del almacenamiento de los documentos en las instalaciones del tercero, dando cumplimiento al control A.15.2.1 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	El Líder del Proceso de Servicios Administrativos evidenció la adecuada definición y asignación del personal para el seguimiento de los contratos supervisados por el Área cumpliendo con el Control A.15.2 1 Seguimiento y revisión de los servicios de los proveedores de la Norma ISO/IEC 27001:2013.

OPORTUNIDADES DE MEJORA

PROCESO	OBSERVACIÓN
PLANEAR	
GESTIÓN INFORMÁTICA	Es pertinente que el proceso de Gestión Informática fortalezca el conocimiento en la administración y mantenimiento de la ruta M para los usuarios finales de los procesos, y así mejorar la utilización de este recurso compartido dando cumplimiento al Control A.12.3.1 Respaldo de la Información de la Norma ISO/IEC 27001:2013.
GESTIÓN DEL RIESGO	Aunque en el Manual de Seguridad de la Información y Ciberseguridad Código GE-NA-FM-041 Versión 8 se detallan en el numeral 3 "objetivos", es pertinente que el Proceso de Gestión del riesgo encargado de liderar el SGSI, realice una clasificación de los mismos a fin de identificar claramente cuáles son los objetivos del manual y cuáles son los del SGSI a fin de establecer los

	criterios que permitan una adecuada medición y apropiación de los mismos. Lo anterior en cumplimiento al numeral 5.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN DEL TRÁMITE	En el formato de Capacitación, se observa que en el registro del 15 de mayo de 2019, se observa que un colaborador asiste, pero no firma el formato de capacitación, por lo cual es pertinente que el proceso controle mejor los documentos de registro, acorde al Control A.7.2.2 de la Norma ISO/IEC 27001:2013.
GESTIÓN DISCIPLINARIA	Toda vez que se publican las capacitaciones de seguridad de la información desde la Oficina de Gestión del Riesgos, se solicita involucrar al personal contratista del proceso de Gestión Disciplinaria, por lo cual es pertinente la participación completa del proceso a fin de dar cabal cumplimiento al control A.7.2.2 de la Norma ISO/IEC 27001:2013.
GESTIÓN JURIDICA	Es fundamental fortalecer el manejo de la herramienta Vigía para mejorar el registro, trazabilidad y seguimiento de los riesgos, acorde al Control A.7.2.2 de la Norma ISO/IEC 27001:2013 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	Es pertinente realizar el fortalecimiento en capacitación a nivel de seguridad de la información y política de protección de datos personales al interior del Área de Servicios Administrativos, a fin de mejorar el cumplimiento del control A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información de la Norma ISO/IEC 27001:2013.

PROCESO	OBSERVACIÓN
HACER	
GESTIÓN DE CONTRATACIÓN	Es pertinente la revisión de la Matriz de Riesgos del proceso donde se identifique los riesgos, causas y controles asociados al proceso y se fortalezca el entendimiento de los mismos dando cumplimiento al Numeral 6.1 Acciones para tratar riesgos y oportunidades de la Norma ISO/IEC 27001:2013.
GESTIÓN DE TESORERÍA	Verificar conjuntamente con el proceso de Gestión del Riesgo, la pertinencia de asociar un riesgo o crear uno

	nuevo frente la custodia de los cheques y documentos de la caja fuerte, verificar causas y controles. Lo anterior en concordancia con el numeral 6.1.2 "valoración de los riesgos de la seguridad de la información" y el Control A.12.1.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE VIVIENDA Y MERCADEO	El proceso de Gestión de Vivienda y Mercadeo envía información vía email, por lo cual es pertinente evaluar la implementación de controles acuerde con la criticidad de la información que se transfiere, lo anterior en cumplimiento al Control A.13.2.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE VIVIENDA Y MERCADEO	En los contratos del proceso de Gestión de Vivienda y Mercadeo se establecen cláusulas de confidencialidad y protección de datos personales, sin embargo, éstas últimas no incluyen el contrato de trasmisión del responsable (Caja Honor) hacia el encargado (contratista), los deberes y la obligación de devolución de la información; razón por la cual se sugiere incluir la autorización de tratamiento de datos personales, los usos que se les va a dar, entre otras el reporte a las centrales de riesgos en caso de un posible incumplimiento, a fin de apoyar el Control A.18.1.4 de la Norma ISO/IEC 27001:2013.
GESTIÓN DE VIVIENDA Y MERCADEO	Actualmente en el proceso de Gestión de Vivienda y Mercadeo no se está llevando un estricto control de seguimiento de las consultas que realizan los funcionarios en las centrales de riesgos, se sugiere implementar el seguimiento requiriendo los reportes al proveedor y comparando contra los trámites de Leasing que se gestionan en el periodo de tiempo, en función al Control A.12.4.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	Se recomienda a la Mesa de Ayuda revisar los casos abiertos en un tiempo prudencial a fin de mejorar y controlar el tiempo entre el cierre y la autorización en la herramienta service manager, en función al Control A.9.2.6 de la Norma ISO/IEC 27001:2013.
GESTIÓN DOCUMENTAL	El proceso de gestión documental funge como custodio del archivo documental de toda la Entidad, ha implementado el flujo documental de "Transferencias documentales" un campo donde el área usuaria debe relacionar que tipo de información (clasificación) está transfiriendo, sin embargo, es necesario fortalecer el

	proceso de identificación, clasificación y etiquetado de la información al interior de la Entidad, para todo tipo de información, a fin de apoyar el cumplimiento del control A.8.1.1 de la Norma ISO/IEC 27001:2013.
GESTIÓN INFORMÁTICA	En el Proceso de Gestión Informática se evidencia el listado de solicitudes por devolución de equipos, es pertinente buscar la viabilidad de adjuntar el reporte de la herramienta service manager para eliminar el papel a fin de apoyar el control A.11.2.7 Disposición segura o reutilización de equipos de la Norma ISO/IEC 27001:2013.
GESTIÓN JURÍDICA	Se recomienda que el Proceso de Gestión Jurídica realice la actualización del registro de activos de información de acuerdo con las recientes novedades de orden institucional, acorde al Control A.8.1.1 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	El conocimiento en el uso de la aplicación de elaboración del carnet y asignación de permisos de acceso a las puertas se encuentra concentrado en un funcionario, por lo cual es pertinente fortalecer la transferencia de conocimiento sobre el proceso en mención dando cumplimiento a los controles A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información y A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	Es pertinente que Servicios Administrativos realice seguimiento semestral con los Líderes de Proceso sobre el control de acceso a oficinas para fortalecer la seguridad de física dando cumplimiento al Control A.11.1.3 Seguridad de oficinas, recintos e instalaciones de la Norma ISO/IEC 27001:2013.

PROCESO	OBSERVACIÓN
VERIFICAR	
ADMINISTRACIÓN DE CUENTAS	Al validar controles implementados por el proceso frente al acceso de información; y de acuerdo con el numeral A.11.1.1 "Perímetro de seguridad física" de la Norma ISO/IEC 27001:2013., se sugiere crear un control para el acceso del archivo documental, el cual hoy se encuentra disponible para los tres

	grupos del área y en el que se evidenció la llave pegada al estante y no con un control de acceso a los documentos. Es por esto, que se recomienda que las llaves sean controladas por cada grupo y se tenga un control de entrada a esta área en la que se almacena los documentos generados por las dependencias.
GESTIÓN INFORMÁTICA	Durante la prueba de recorrido en el proceso de Gestión de Contratación se evidencio que un equipo de cómputo permitió el acceso al panel de control, opción que es restringida para los usuarios y que luego de los mantenimientos preventivos y correctivos a los equipos de cómputo de Caja Honor quedan accesos directos a las herramientas de apoyo de Mesa de Ayuda por lo cual es pertinente que la Oficina Asesora de Informática, valide los accesos restringidos, esto en cumplimiento al control A.9.4.4 Uso de los programas utilitarios privilegiados de la Norma ISO/IEC 27001:2013.
GESTIÓN DE VIVIENDA Y MERCADEO	Se procedió con la revisión de los accesos a carpeta compartida en el proceso de Gestión de Vivienda y Mercadeo. Por lo anterior se requiere evaluar la criticidad de la información que se genera en el área, a fin de que el proceso gestione al interior de manera más eficiente los controles con los que cuenta en cumplimiento al Control A.9.2.5 de la Norma ISO/IEC 27001:2013.
GESTIÓN DOCUMENTAL	Al revisar el índice de información clasificada y reservada de la Entidad del proceso de Gestión Documental, no se logró identificar activos de información que tengan que ver con la información personal de los afiliados, por lo cual es pertinente aplicar una clasificación de frente al control A.8.2.1 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	Acorde con las normas de gestión documental expedidas por el Archivo General de la Nación, los extintores permitidos en el área de gestión documental son multipropósito o Solkaflam, sin embargo, en el área principal de gestión documental se encontró un extintor de agua a presión, lo cual no permitiría reaccionar efectivamente ante un incidente causado por una

	amenaza ambiental, por lo cual es pertinente la revisión de todos los extintores de la entidad, en atención al control A.11.1.4 de la Norma ISO/IEC 27001:2013.
SERVICIOS ADMINISTRATIVOS	Es oportuno fortalecer la política de Seguridad física y del entorno para los equipos portátiles, debido a que en la prueba de recorrido se evidenció 2 portátiles (uno con la clave predispuesta y el otro sin guaya visible), lo anterior a fin de apoyar el cumplimiento de la Norma ISO/IEC 27001:2013, Control A.11.2.1 Ubicación y protección de los equipos.
GESTIÓN INFORMÁTICA	Se recomienda a la Mesa de Ayuda del proceso de Gestión Informática fortalecer la revisión de la activación del S.O en el alistamiento de equipo a entregar a los procesos para minimizar el riesgo que se pueda presentar en los equipos con el paquete ofimático entregado, a fin de mejorar el cumplimiento de la Norma ISO/IEC 27001:2013, Control A.18.1.2 Derechos de propiedad intelectual.

PROCESO	OBSERVACIÓN
ACTUAR	
GESTIÓN DEL RIESGO	Se recomienda por parte de la Oficina Asesora de Gestión del Riesgo, reforzar el uso del formato de confidencialidad para el uso de dispositivos móviles y acceso remoto a los líderes que realicen uso de estos servicios, a fin de mejorar el cumplimiento al Control A.6.2.1 Política para dispositivos móviles de la Norma ISO/IEC 27001:2013.
GESTIÓN DEL SAC	Se verifica el flujo del PQRD totalmente automatizado, sin embargo a los autorizados a nivel consulta se recomienda realizar un levantamiento de roles específico en el PQRD, por parte de todos los procesos de la Entidad, con el fin de continuar con el cumplimiento de los Controles A.18.1.3 Protección de registros y A.18.1.4 Privacidad y Protección de información de datos personales de la Norma ISO/IEC 27001:2013

GESTIÓN DISCIPLINARIA	El proceso de Gestión Disciplinaria toma las fotocopias en el área de atención al afiliado, aunque la destrucción de la información se hace de manera manual, dando cumplimiento al control A.8.3.1 de la Norma ISO/IEC 27001:2013., aunado a lo anterior es pertinente evaluar la adquisición de una destructora de papel dada la criticidad de la información que se gestiona en el área.
GESTIÓN DOCUMENTAL	El sistema de información Workmanager, tiene establecidos roles de acuerdo a cada tipo de área en la que se desempeña cada funcionario, sin embargo, es oportuno fortalecer la segregación de funciones y roles en el sistema de información Workmanager, para que los líderes de los procesos conozcan hasta que información tiene acceso él y sus colaboradores, lo anterior en cumplimiento al Control A.9.4.1 de la Norma ISO/IEC 27001:2013.

CONCLUSIONES

De acuerdo con el Plan de Auditoría, se observa que se cumplieron los objetivos en el mismo, dentro del alcance y criterios determinados. En las auditorías efectuadas en los procesos que se encontraban dentro del alcance, se evidenciaron Oportunidades de Mejora que deben ser tratadas y mitigadas por las áreas correspondientes de manera autónoma, así mismo se generaron NC, que se requieren sean gestionadas de manera inmediata por los líderes responsables, para garantizar el cumplimiento de la Norma ISO 27001:2013.

Cordialmente,

JHON JAIRO ROSAS ALBA
Jefe Oficina Asesora de Gestión del Riesgo

Proyectó y elaboró
Luis Carlos Rivera Torrenegra
Auditor Líder ISO27001:2013