INFORME DE AUDITORÍA INTERNA	

TIPO DE AUDITORÍA	Auditoría SCI
FECHA DEL INFORME	2022-12-26
FECHA DE LA AUDITORÍA	2022-08-19
Lugar	Bogotá

LÍDER DE PROCESO
Nombre - Cargo / Dependencia
Luis Ariel Prieto Lemus - DIRECTOR TECNOLOGIA
COLABORADORES QUE ATENDIERON LA AUDITORÍA
Nombre - Cargo / Dependencia
Carlos Eduardo Cruz Gonzalez - ANALISTA TECNOLOGIA
Colaboradores adicionales
Patricia Londoño Garcia Maria Claudia Calixto Medrano.

EQUIPO AUDITOR
Nombre - Cargo / Dependencia
Marlon Rene Castro Salcedo - CONTRATISTA OCI

PROCESOS	• Gestión de Servicios Tecnológicos
PROCESO, PROCEDIMIENTO O ACTIVIDAD A AUDITAR	Gestión de Servicios Tecnológicos
OBJETIVO DE LA AUDITORÍA	Analizar, verificar y evaluar la funcionalidad y seguridad de los sistemas de información CORE, C&CTEX y Kactus.
ALCANCE	Verificación de la funcionalidad de los aplicativos en el periodo comprendido entre el 1 de enero y el 30 de julio de 2022.
CRITERIOS	Ley 87 de 1993, por lo cual se establecen las normas para el ejercicio del control interno en la entidades y organismos del estado y se dictan otras dispocisiones. Decreto 1499 de 2017, por medio del cual se modifica el decreto 1083 de 2015, decreto único reglamentario del sector función pública, en lo relacionado con el sistema de gestión establecido en el articulo 133 de la ley 1753 de 2015. Procedimiento gestión de incidentes código A7-1-13 versión 3. Procedimiento gestión de accesos y retiro de servicios A7-1-05 versión 12.
FORTALEZAS	

HALLAZGOS			
CRITERIO DE AUDITORÍA	**TIPO**	**DESCRIPCIÓN**	**RECOMENDACIÓN**
Gestión de incidentes • Procedimiento	Observación de mejora	Se evidencia en el caso No. 472, que no se está realizando el cierre del caso una vez es solucionado por el ingeniero a cargo, de acuerdo con el registro en la herramienta ARANDA, el administrador fue quien se encargó de documentar y dar cierre al caso creado para el sistema de información C&CTEX.	Se recomienda a la Dirección de Tecnología fortalecer los controles para garantizar el cumplimiento de los acuerdos de niveles de servicio con el proveedor e implementar acciones efectivas de mitigación para un cierre oportuno, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de incidentes • Procedimiento	Observación	Se evidenció falla en el sistema de informacion CORE (evento de riesgo 2872), lo cual ocasionó permitir la generación de registros con más de una solicitud por vigencia, es decir, un beneficiario sólo puede tener un crédito de la línea tradicional adjudicado o en progreso de otorgamiento.	Se recomienda a la Dirección de Tecnología rediseñar y fortalecer los controles existentes con el propósito que se brinde un plan de

			acción consistente y se atienda oportunamente el riesgo materializado en el aplicativo C&CTEX.
Gestión de incidentes • Procedimiento	Observación	Se identificó incumplimiento en los Acuerdos de nivel de servicio para la solución de incidentes en el sistema de información CORE, lo anterior luego de analizar 114 casos con prioridad media, alta y critica detectando que superan el tiempo estipulado según la prioridad.	Se recomienda a la Dirección de Tecnología rediseñar y fortalecer los controles existentes, además de establecer un plan de acción con un adecuado análisis de causas efectivas para la mitigación del caso, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de incidentes • Procedimiento	Observación	Se evidencia en el historial para la gestión de problemas que los incidentes que más se presentan son: bloqueo de usuarios, fallas en la conectividad a la VPN, falla en equipo de cómputo y falla en la consulta y modificación, demostrando que es necesario implementar acciones para mitigar los incidentes más reportados por los usuarios.	Se recomienda a la Dirección de Tecnología fortalecer los acuerdos de niveles de servicio con el proveedor y establecer un plan de accion con un adecuado analisis de causas efectivas para la mitigación de los casos más recurrentes reportados por los usuarios, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de incidentes • Procedimiento	Observación	Se evidencia falla en el sistema de información C&CTEX (evento de riesgo 2837), lo cual genera que algunos campos presenten caracteres no correspondientes a la información requerida, que la estructura de las direcciones no sea la correcta o no tenga la información correspondiente al campo, registros con el mismo número de identificación, nombres y apellidos errados, número y tipo de identificación errados, lo anterior, afectando la generación del informe de exógenas correspondiente a la cartera que debe ser entregado a la DIAN, así mismo, toda comunicación que sea remitida a los beneficiarios puede tener un alto riesgo de envío con información errada o a la dirección de correspondencia equivocada.	Se recomienda a la Dirección de Tecnología rediseñar y fortalecer los controles existentes, establecer un plan de acción con un adecuado análisis de causas efectivas para la mitigación del riesgo, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de incidentes • Procedimiento	Observación	Se evidencian 213 incidentes que no cumplen con los acuerdos de niveles de servicios para la solución de incidentes tipificados con prioridad alta para el sistema de información C&CTEX.	Se recomienda a la Dirección de Tecnología rediseñar y fortalecer los controles existentes, establecer un plan de acción con un adecuado análisis de causas efectivas de mitigación con el objetivo cumplir con los tiempos de respuesta estipulados para los incidentes.
			Se recomienda a la Dirección de Tecnología fortalecer los controles para garantizar el cumplimiento de los acuerdos de

Gestión de incidentes • Procedimiento	Observación	Se evidencian 47 incidentes tipificados con prioridad alta y baja que no cumplen con los acuerdos de niveles de servicios para la atención de incidentes para el sistema de información C&CTEX.	niveles de servicio con el proveedor e implementar acciones efectivas de mitigación de los casos más recurrentes reportados por los usuarios, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de incidentes Gestión de Servicios Tecnológicos	Observación	En el historial de incidentes para el periodo de enero a julio para los sistemas de información C&CTEX se evidencia que el incidente que más se presenta es el de bloqueo de usuarios, demostrando que es necesario implementar acciones para mitigar el problema.	Se recomienda a la Dirección de Tecnología implementar acciones efectivas de mitigación de los casos más recurrentes reportados por los usuarios, con el objetivo de bajar el índice de fallas recurrentes en los sistemas de información.
Gestión de incidentes • Procedimiento	Observación	Se evidencian 21 incidentes que no cumplen con los acuerdos de niveles de servcio para la solución de incidentes estipulados para el sistema de información KACTUS.	Se recomienda a la Dirección de Tecnología fortalecer los controles para garantizar el cumplimiento de los acuerdos de niveles de servicio con el proveedor e implementar acciones efectivas de mitigación de los casos más recurrentes reportados por los usuarios, con el objetivo cumplir con los tiempos de respuesta a las fallas persistentes y permanentes en los sistemas de información.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se evidencian seis (6) usuarios con contrato finalizado y activos para CORE Signature. Captura de Pantalla 2022-09-30 a la(s) 5.10.15 p. m..png (62 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital numeral 9.3 “Política de Desvinculación, Licencias, Vacaciones o Cambio de Labores de los Funcionarios y Personal Provisto por Terceros”, monitoreando y reportando de maneara inmediata la desvinculación o cambio de labores de funcionarios y contratistas, fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas, con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente verificación de la Oficina de Riesgos.
			Se recomienda a la Dirección de

Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se evidencia un (1) usuario con contrato finalizado y activo en el sistema de información CORE SAC: Captura de Pantalla 2022-09-30 a la(s) 5.09.10 p. m..png (20 KB) 	Tecnología dar cumplimiento a la política de seguridad digital numeral 9.3 “Política de Desvinculación, Licencias, Vacaciones o Cambio de Labores de los Funcionarios y Personal Provisto por Terceros”, monitoreando y reportando de maneara inmediata la desvinculación o cambio de labores de funcionarios y contratistas, fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas, con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente verificación de la Oficina de Riesgos.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se evidencian cuatro (4) usuarios con contrato finalizado y activos en el sistema de información CORE SM: Captura de Pantalla 2022-09-30 a la(s) 5.08.07 p. m..png (44 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital numeral 9.3 “Política de Desvinculación, Licencias, Vacaciones o Cambio de Labores de los Funcionarios y Personal Provisto por Terceros”, monitoreando y reportando de maneara inmediata la desvinculación o cambio de labores de funcionarios y contratistas, fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas, con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente verificación de la Oficina de Riesgos.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se evidencian 3 (tres) usuarios con contrato finalizado y activos en el sistema de información C&CTEX. Captura de Pantalla 2022-09-30 a la(s) 5.06.51 p. m..png (37 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital numeral 9.3 “Política de Desvinculación, Licencias, Vacaciones o Cambio de Labores de los Funcionarios y Personal Provisto por Terceros”, monitoreando y reportando de maneara inmediata la desvinculación o cambio de labores de funcionarios y contratistas, fortalecer los controles

			existentes y establecer un plan de acción con un adecuado análisis de causas efectivas, con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente verificación de la Oficina de Riesgos.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se evidencian 12 (doce) usuarios en estado activo y con varias cuentas en el sistema de información CORE SM. Captura de Pantalla 2022-09-30 a la(s) 4.53.03 p. m..png (223 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital Numeral 11.5 Política de Control de Acceso a Sistemas Y Aplicativos "...ICETEX vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información...". "...Normas dirigidas a: OFICINA DE RIESGOS Revisar la creación o modificación de los perfiles que acceden a los recursos tecnológicos y sistemas de información del instituto..." fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente revisión de la Oficina de Riesgos.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se identificaron 5 (cinco) usuarios en estado activo y con varias cuentas en el sistema de información CORE SAC. Captura de Pantalla 2022-09-30 a la(s) 4.56.54 p. m..png (74 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital Numeral 11.5 Política de Control de Acceso a Sistemas Y Aplicativos "...ICETEX vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información...". "...Normas dirigidas a: OFICINA DE RIESGOS Revisar la creación o modificación de los

			perfiles que acceden a los recursos tecnológicos y sistemas de información del instituto...” fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente revisión de la Oficina de Riesgos.
Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Se identificaron 12 (doce) usuarios en estado activo y con varias cuentas, para 2 (dos) usuarios los documentos registrados no corresponden a números de cédulas, estos casos se detectaron en el sistema de información CORE Signature. Captura de Pantalla 2022-09-30 a la(s) 4.58.52 p. m..png (155 KB) 	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital Numeral 11.5 Política de Control de Acceso a Sistemas Y Aplicativos “...ICETEX vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información...”. “...Normas dirigidas a: OFICINA DE RIESGOS Revisar la creación o modificación de los perfiles que acceden a los recursos tecnológicos y sistemas de información del instituto...” fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la correspondiente revisión de la Oficina de Riesgos.
		Se identificaron 3 (tres) usuarios en estado activo y con varias cuentas, en el sistema de información C&CTEX.	Se recomienda a la Dirección de Tecnología dar cumplimiento a la política de seguridad digital Numeral 11.5 Política de Control de Acceso a Sistemas Y Aplicativos “...ICETEX vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen

Gestión de accesos y retiro de servicios Gestión de Servicios Tecnológicos	Observación	Captura de Pantalla 2022-09-30 a la(s) 5.00.57 p. m..png (47 KB) 	conforme a los niveles de acceso a la información...". "...Normas dirigidas a: OFICINA DE RIESGOS Revisar la creación o modificación de los perfiles que acceden a los recursos tecnológicos y sistemas de información del instituto..." fortalecer los controles existentes y establecer un plan de acción con un adecuado análisis de causas efectivas con el objetivo de subsanar las debilidades evidenciadas en vista de ser un caso recurrente y con la corresponiente revisión de la Oficina de Riesgos.
Gestión de backups Gestión de Servicios Tecnológicos	Observación	Se evidencia en el sistema de información C&CTEX que uno de los backup finalizó con estado fallido en los meses de enero de 2022. Se realizó el relanzamiento del backup con resultado fallido en cuatro intentos.	Se recomienda a la Dirección de Tecnología verificar que las políticas de ejecución definidas en el procedimiento de gestión de backup del proveedor sean ejecutadas y su resultado sea exitoso. Se recomienda documentar el relanzamiento del backup en caso de falla de la ejecución, teniendo en cuenta el procedimiento de administración de backup del contratista.
Gestión de backups • Procedimiento	Observación	Se evidencia en el sistema de información kactus que algunos backups finalizaron con estado fallido en los meses de febrero y abril de 2022. No se evidenció el relanzamiento de backup.	Se recomienda a la Dirección de Tecnología verificar que las políticas de ejecución definidas en el procedimiento de gestión de backup del proveedor sean ejecutadas y su resultado sea exitoso. Se recomienda documentar el relanzamiento del backup en caso de falla de la ejecución, teniendo en cuenta el procedimiento de administración de backup del contratista.

CONCLUSIONES DE LA AUDITORÍA (aplica para sistemas de gestión)	

Firmas	Nombre	Cargo	Fecha
Auditor	Marlon Rene Castro Salcedo	CONTRATISTA OCI	2022-09-30 17:42:43
Aprobador	Jose Jaime Beltran Arias	COORDINADOR OCI	2022-10-04 07:40:33
Aprobador	Carlos Javier Rodríguez Ordoñez	JEFE DE OFICINA OCI	2022-12-16 10:22:39