Entidad
Inspección No. 17-07-03-00-19
Fecha de elaboración

1. Identificación y descripción del Hallazgo

ID del hallazgo :

En los sistemas de información Charry y Mantis y el servicio de directorio activo no se garantiza la administración segura de roles y privilegios, ni los principios de no repudio, y de mínimo privilegio. Lo anterior se evidencia en que: i) no se cuentan con lineamientos e instrumentos para crear, actualizar, inactivar y hacer seguimiento a los roles y privilegios asignados.; ii) en el ingreso no autorizado a una estación de trabajo; iii) en la falta de configuración de logs de auditoria sobre el servidor de directorio activo. Por lo anterior, las actividades de los usuarios en dichos aplicativos no se puede auditar y ante posibles escenarios de pérdida de confidencialidad, integridad y disponibilidad de la información, la entidad no tiene la posibilidad de identificar los responsables directos de dichas acciones. Lo anterior, va en contravía de lo dispuesto en: i) modelo de seguridad de la información SANSI PS1 principio del mínimo privilegio y gestión de identificadores; ii) el SM4.4.4 Gestión de Identidad y acceso / administrar los privilegios de acceso de usuario; iii) la ISO 27001 numeral A19.1.3 Distribución de funciones, A11.5.2 Identificación y autenticación de usuarios, A11.6.1 Restricción del acceso a la información, A 10.10.1 Registro de auditorias y Política de uso de contraseñas y Gestión de contraseñas para usuarios; y en iV) la política de seguridad de Coljuegos numeral 3.4 Políticas de servicios de red.

2. Identificación de los Riesgos que se mitigan

ID del Riesgo de Gestión : RGSITRC001-RGSITRC009

RG01.
Desalineación entre las funciones del cargo y los roles y privilegios

RG02.
Discrecionalidad en la creación de roles y privilegios

RG03.
Pérdida de la trazabilidad de los eventos de los sistemas de información

RG04.
Inadecuado uso de contraseñas

RFC 01.
Exposición de la información

RFC02.
Pérdida de efectividad y eficiencia en el control tributario

3. Descripción del Plan de prevención de fraude y corrupción

ID	3.1 Acciones	3.2 Tipo de acción	3.3 Objetivo	3.4 Meta		3.5 Fecha inicio meta	3.6 Fecha fin meta	3.7 Área responsable	AVANCES
				Cantidad	Producto				
1	Definir una politica para informar a TIC sobre las novedades que se presenten de personal que permitan depurar los roles y privilegios	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	1	Politica incluida en el macroproceso de Capital Humano	01/04/2015	30/04/2015	Capital Humano y TIC	Se incluyó la política 5.10 "Las novedades de administración de personal (ingresos, traslados, egresos, vacaciones, licencias maternidad/paternidad, comisiones, licencias No remuneradas superiores a 3 dias e incapacidades superiores a 3 dias), deberán ser informadas al área de Tic´s a través de la herramienta mesa de ayuda, con el fin que se tomen las acciones correspondientes a la gestión de cuentas de usuario."en las POLÍTICAS MACRO PROCESO CAPITAL HUMANO (Código: GCH-RE-01, versión 3- Vigencia: 13/Jul/2015) **CUMPLIDO**
2	Definir una política de registro y monitoreo de log de auditoría y realizar una revisión por semestre.	Preventivo	Disponer de información de trazabilidad de las operaciones que realizan los usuarios de Coljuegos	1	Politica incluida en el macroproceso de TIC	01/04/2015	30/04/2015	TIC	Se incluyó la siguiente política en el documento POLÍTICAS MACRO PROCESO GESTIÓN DE TIC (Código: TIC-RE-01, Vigencia: 28/May/2015) "1.3. ENTREGAR SOPORTE Se deberán registrar y monitorear los logs de auditoría de los sistemas de información y aplicaciones, bases de datos, sistemas operativos y firewall y realizar una revisión semestral a los mismos." **CUMPLIDO**
3	Documentar para cada aplicación (ORFEO, SIPLAFT, MET, SIITO, SIICOL Y MANTIS) - La definición de roles - El responsables funcional de autorizar los roles para cada aplicación - El responsable técnico de verificar la implementación en cada aplicativo de los roles que se requieran	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	6	Documento para cada aplicación, con los roles definidos	01/04/2015	30/09/2015	Financiera y Administrativa : SIICOL y ORFEO Gestión Contractual: SIPLAFT, MET, SIITO TIC: MANTIS	**EN PLAZO** Avance: Se definió la matriz de roles y perfiles para ORFEO, SIPLAFT, MET, SIITO, y SIICOL.
4	Actualizar el documento de Gestion de cuentas de usuarios, de tal forma que se incluya: - Lineamientos y Procedimientos para la administración (creación, actualización e inactivación) de usuarios de servicios informáticos, entre otras para las aplicaciones de ORFEO, SIPLAFT, MET, SIITO, SIICOL Y MANTIS. - Política para la depuración de usuarios, que determine las directrices para la modificación e inactivación de usuarios. Dicha depuración debe aplicarse por lo menos una vez al año para las aplicaciones: ORFEO, SIPLAFT, MET, SIITO, SIICOL Y MANTIS.	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	1	Instructivo Gestión de cuentas de usuarios	01/04/2015	30/09/2015	Financiera y Administrativa : SIICOL y ORFEO Gestión Contractual: SIPLAFT, MET, SIITO TIC: MANTIS	**EN PLAZO**
5	Gestionar los recursos presupuestales necesarios para adquirir un software para el registro y control de los roles y privilegios asociados a cada funcionario.	Preventivo	Disponer de información de trazabilidad de las operaciones que realizan los usuarios en los aplicativos de Coljuegos	1	Solicitud soportada con estudio de mercado	01/06/2015	31/07/2015	TIC	**EN PLAZO** Tics afirma que: *"Debido a recortes presupuestales no es posible adquirir en la presente vigencia, el software para el registro y control de los roles y privilegios asociados a cada funcionario. Sin embargo se está trabajando en la integración de los sistemas de Información con el directorio activo, para que se ingrese con el mismo usuario y contraseña a estos sistemas. Se tiene integrados a la fecha, la intranet, Isolución, Orfeo, SIICOL y Mantis. Se está delantando con el proveedor la integración de SARA al directorio activo también."* A 30 de Junio de 2015, la OCI, no evidenció las gestiones realizadas respecto los recursos presupuestales necesarios para adquirir un software para el registro y control de los roles y privilegios asociados a cada funcionario, soportados con estudio de mercado

ID	3.1 Acciones	3.2 Tipo de acción	3.3 Objetivo	3.4 Meta		3.5 Fecha inicio meta	3.6 Fecha fin meta	3.7 Área responsable	AVANCES
				Cantidad	Producto				
6	Habilitar, configurar y diseñar un monitoreo para el registro de eventos del servidor de dominio.	Preventivo	Disponer de información de trazabilidad de las operaciones que realizan los usuarios en los aplicativos de Coljuegos	1	Informes de revisión de eventos del servidor de dominios	01/04/2015	30/06/2015	TIC	**Avance:** Tics afirma que: "*Se activó el log de eventos de seguridad del servidor controlador de dominio. Se han venido guardando los logs.* *Estado:* *En la actualidad Coljuegos realiza captura y almacenamiento de los archivos de log de su directorio activo, y son almacenados en la unidad de SAN. Sin embargo aun no cuenta con un software de syslog que permita ejecutar auditorias sobre dichos archivos y el análisis de cada uno de ellos, es una tarea altamente dispendiosa, dado que se trata de archivos de mas de 250.000 registros.* *Respecto la documentación del monitoreo, esta pendiente elaborar un monitoreo para una persona que haya salido de vacaciones, licencias de maternidad, licencias no remuneradas"* De acuerdo a la revisión realizada por la OCI, estan pendientes las evidencias del monitoreo. **PENDIENTE**
7	Implementar los sistemas de alertas y logs que poseen el Directorio activo, System Center Configuration Manager, System Center Dataprotection Manager y Fortinet. Diseñar un monitoreo al respecto.	Preventivo	Disponer de información de trazabilidad de las operaciones que realizan los usuarios en los aplicativos de Coljuegos	1	Informes de alertas DA, SCCM, SCDP, Fortinet	01/07/2015	31/09/2015	TIC	**EN PLAZO**
8	Realizar auditorías y monitorear los controles implementados en la gestión de acceso de usuario y la gestión de privilegios para las aplicaciones:ORFEO, SIPLAFT, MET, SIITO, SIICOL Y MANTIS.	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	1	Informes de revisión de roles y pefiles	01/04/2015	31/12/2015	TIC	**EN PLAZO**
9	Realizar sensibilizaciones de las políticas de seguridad, donde se indique los efectos disciplinarios del descuido de las contraseñas y tokens.	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	2	Difusión por Correo e Intranet	01/04/2015	31/09/2015	TIC y Comunicaciones	**EN PLAZO**
10	Generar un listado de eventos criticos para SIICOL y ORFEO	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de iformación de Coljuegos	1	Listado de eventos criticos para SIICOL y ORFEO	01/11/2015	31/12/2015	Desarrollo de Mercados, Gestión Contractual y Administrativa y Financiera	**EN PLAZO**
11	Implementar en SIICOL un log de auditoría y sistema de alertas de aquellas operaciones críticas para Coljuegos	Preventivo	Disponer de información de trazabilidad de las operaciones que realizan los usuarios de SIICOL	1	Software para log de auditoria y alertas	01/11/2015	31/12/2015	TIC	**EN PLAZO**
12	Generar informes a la Gerencia de TIC sobre el comportamiento de los soportes de TIC registrados en la herramienta Mantis	Correctivo	Mejorar la atención a los usuarios internos de Coljuegos	12	Informes de solicitudes de soporte	01/01/2015	31/12/2015	TIC	**EN PLAZO** **Avance:** Se han generado 6 informes sobre el comportamiento de los soportes de TIC registrados en la herramienta Mantis
13	Generar informe de trazabilidad de PQRD a traves de Orfeo	Correctivo	Mejorar los tiempos de respuesta a las PQRD	2	Informes de trazabilidad de PQR	01/07/2015	31/12/2015	Juridica	**EN PLAZO:** **Avance:** Mediante correo electrónico del 29 de abril de 2015, se infomó a los funcionarios de Coljuegos, sobre los siguientes desarrollos de orfeo: • Pre-Radicaciónpor parte de las áreas – Radicación definitiva por parte del Área de Correspondencia. • Usuarios Líder de PQRD • Informes de trazabilidad de radicados • Alarmas de vencimientos de radicados y PQRD • Activación de conexión automática a Orfeo a través del ingreso a la intranet C-Innova • Webservices de integración de Orfeo con la planta telefónica Elastix – Herramienta para Servicio al Cliente únicamente.

Código	PM01-AGR-PR03-FT03	Versión:	1	Fecha de emisión:	