



Entidad  
Inspección No.  
Fecha de elaboración

COLJUEGOS  
17-07-03-00-19

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 auditoría 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 contra de lo dispuesto en: i) modelo de seguridad de la información SANSI FSI principio del mínimo privilegio y gestión de identificadores; ii) el SMA 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 auditorías 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 :

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	3.8 Nombres y apellidos - cargo	Avance al 30 de junio de 2016
				Cantidad	Producto					
1	Definir una política 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 información de Coljuegos	1	Política incluida en el macroproceso de Capital Humano	01/04/2015	30/04/2015	Capital Humano y TIC	Ingeniero de calidad y seguridad	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 días e incapacidades superiores a 3 días), 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) <b>CUMPLIDO 100%</b>
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	Política incluida en el macroproceso de TIC	01/04/2015	30/04/2015	TIC	Ingeniero de calidad y seguridad	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." <b>CUMPLIDO 100%</b>
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 requirieran	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de información 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	VGC, VDO, Lider ORFEO, Profesional VGC, Lider SIITO, - Lider Seguridad y Calidad de la información	Matrices actualizadas al 30-09-2015 de roles y perfiles para ORFEO, SIPLAFT, MET, SIITO, y SIICOL. <b>CUMPLIDO 100%</b>
4	Actualizar el documento de Gestión 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 información 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	VGC, VDO, Lider ORFEO, Profesional VGC, Lider SIITO, - Lider Seguridad y Calidad de la información	Se aprobó el instructivo Gestión de cuentas de usuarios en su versión No.02. Soportes enviados al ITRC en reporte a 31 de diciembre de 2015. <b>CUMPLIDO 100%</b>



Entidad  
Inspección No.  
Fecha de elaboración

COLJUEGOS  
17-07-03-00-19

1. Identificación y descripción del Hallazgo

ID del hallazgo :

En los sistemas de información Chary 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 auditoría 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 PSI principio del mínimo privilegio y gestión de identificadores; ii) el SMA.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 auditorías 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 :

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	3.8 Nombres y apellidos - cargo	Avance al 30 de junio de 2016
				Cantidad	Producto					
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	Ingeniero de Seguridad y Calidad	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. <b>CUMPLIDO 100%</b>
6	Habilitar, configurar y diseñar un monitoreo para el registro de eventos del servidor de dominio. En Reunión del día 03-07-2015 en Coljuegos se definió documentar el monitoreo(Pasos seguidos y resultados).	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	- Ingeniero redes y comunicaciones	Conforme con lo acordado en reunión con el ITRC se elaboró el documento de los pasos para realizar el monitoreo. <b>CUMPLIDO 100%</b>



Entidad  
Inspección No.  
Fecha de elaboración

COLJUEGOS  
17-07-03-00-19

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 auditoría 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 auditorías 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 :

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	3.8 Nombres y apellidos - cargo	Avance al 30 de junio de 2016
				Cantidad	Producto					
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	Ingeniero redes y comunicaciones/Ingeniero Soporte	En la actualidad Coljuegos realiza captura y almacenamiento de los archivos de log de System center (Configuration Manager) el cual son respaldados en los visores de eventos de cada servidor. Se están respaldando en un servidor externo en las siguientes rutas: \\10.117.100.14\LOGS_CONFIGURATION MANAGER y \\10.117.100.14\LOGS_DPM, la aplicación Configuration manager genera sus propias alertas las cuales son monitoreadas todos los días, en la ruta de (supervisión-Alertas). <b>CUMPLIDO 100%</b>
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. En Reunión del día 03-07-2015 en Coljuegos se definió que finalizada esta tarea informar a los jefes para su aprobación.	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de formación de Coljuegos	1	Informes de revisión de roles y perfiles	01/04/2015	31/12/2015 Reprogramado para el 30-06-2016	TIC	Ingeniero de Seguridad y Calidad	Se realizó auditoría y monitoreo a los controles implementados en la gestión de acceso de usuario y la gestión de privilegios para la aplicación MET-SCLM-ORFEO-SIPLAFT-SIITO-SIICOL. Para lo anterior se evidencian soportes de informes de auditoría. Se anexan soportes. <b>Cumplido 100%</b>
9	Realizar sensibilizaciones de las políticas de seguridad, donde se indique los efectos disciplinarios del descuido de las contraseñas y tokens. En Reunión del día 03-07-2015 en Coljuegos, ITRC considera que en el Tapiz ir colocando una política cada día.	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de formación de Coljuegos	2	Difusión por Correo e Intranet	01/04/2015	31/09/2015	TIC y Comunicaciones	Ingeniero de Seguridad y Calidad, Profesional Comunicaciones	Desde el día 17-09-2015 se publicó en c-innova la política de seguridad de la información y la explicación de los principios de Confidencialidad, Integridad y Disponibilidad, para la consulta de los funcionarios de Coljuegos. <b>CUMPLIDO 100%</b>
10	Generar un listado de eventos críticos para SIICOL y ORFEO	Preventivo	Reducir el riesgo de fraude, corrupción o fuga, con la información que se registra en los sistemas de formación de Coljuegos	1	Listado de eventos críticos para SIICOL y ORFEO	01/11/2015	31/12/2015 Reprogramado para el 30-06-2016	Oficina Jurídica, Gestión Contractual y Administrativa y Financiera	Jefe Oficina Jurídica, VGCC, Bernardo Becerra - Gerente Administrativo y Financiero	Se genero listado de eventos críticos para SIICOL y Orfeo Se evidencia soportes como son archivo de excel de Levantamiento de Informacion Modulo de auditoria y Acta de reunion indentificando eventos criticos y logs de auditoria de SIICOL. Se anexan soportes. <b>Cumplido 100%</b>

Entidad  
Inspección No.  
Fecha de elaboración

COLJUEGOS  
17-07-03-00-19

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 auditoría 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, A10.10.1 Registro de auditorías 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 :

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	3.8 Nombres y apellidos - cargo	Avance al 30 de junio de 2016
				Cantidad	Producto					
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 auditoría y alertas	01/11/2015	31/12/2015 Reprogramado para el 30-06-2016	TIC	Lider SIICOL	Se elaboró el software de auditoría y las pruebas correspondientes Se evidencia la elaboración de acta de liberación del modulo de auditoría y acta de prueba de logs. Se anexan soportes. <b>Cumplido 100%</b>
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	Ingeniero de Seguridad y Calidad	Soportes enviados al ITRC en reporte a 31 de diciembre de 2015. <b>CUMPLIDO 100 %</b>
13	Generar informe de trazabilidad de PQRD a través de Orfeo	Correctivo	Mejorar los tiempos de respuesta a las PQRD	2	Informes de trazabilidad de PQR	01/07/2015	31/12/2015	Jurídica	Corredor Tecnico Gerencia Administrativa	Se adjunta informe de PQRD's para el periodo julio a diciembre de 2015. Soportes enviados al ITRC en reporte a 31 de diciembre de 2015. <b>CUMPLIDO 100%</b>