

MEMORANDO

Bogotá D.C., 30 de Abril de 2018



UPRA Unidad de Planificación Rural Agropecuaria

Al contestar cite este número: 2018-3-001429

Fecha: 2018-04-30 17:04 Folios: folios Anexos: NO
Trámite: AUDITORIA_INTERNA–Auditoria interna
Tipo doc: OF–Oficio
Remitente: 0102–Dir. Gral - Asesoría de Control Interno
Destinatario: 02-Oficina TIC
Clasificación: Publico

PARA: Daniel Mauricio Rozo
Jefe Oficina TIC

DE: Asesoría de Control Interno

ASUNTO: Remisión de informe final de auditoría

Reciba un cordial saludo,

Con el presente se remite el informe final de auditoría de gestión realizada al proceso de Gestión de Información y Conocimiento con el objetivo de verificar efectividad de controles del Sistema de Seguridad de la Información.

Atentamente,



Sandra Milena Ruano Reyes

Asesor Control Interno

Adjunto: Doctor Felipe Fonseca Fino, Director General
Anexo:

Elaboró: Sandra Milena Ruano Reyes
Revisó: --

Objetivo:

Verificar la efectividad de controles del Sistema de Gestión de Seguridad de Información aplicados en el Proceso de Gestión de Información y Conocimiento GIC-PR-001

Alcance:

Verificación de una muestra de controles definidos en la declaración de aplicabilidad y aplicados durante la vigencia de 2017 y los controles de los riesgos de gestión relacionada con el objeto de la auditoria.

Criterios de auditoria:

NORMA ISO 27002, Modelo de Seguridad y Privacidad de la Información del MINTIC

Riesgos y controles:

Se evaluaron los controles del Mapa de Riesgos del Proceso de Gestión de Información y Conocimiento

Conclusión:

El SGSI en la Upra presenta un avance en su implementación acorde con los plazos establecidos en el Decreto 1078. Se puede concluir que la entidad ha tomado las medidas pertinentes para la implementación del SGSI.

Hallazgos, oportunidad de mejora, identificadas y observaciones:

OBSERVACIÓN			
Nº	Descripción	Riesgo, Impacto, Categoría	Recomendación
1	<p>12. SEGURIDAD EN LA OPERATIVIDAD</p> <p>12.1.2 Gestión de Cambios</p> <p>Se evidencia que para los cambios de software que registran en el módulo de asistencia técnica de SEA, falta de completitud en la información de seguimiento lo cual no permite dejar traza de la descripción del cambio que se generó, Del listado de 268 incidencias reportadas por los usuarios durante el periodo del 1 de enero a abril de 2018 se evidencia que no se puede identificar de forma eficiente cuales generaron cambios a</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Se recomienda fortalecer las actividades de supervisión del líder del proceso con el fin de asegurar la ejecución del 100% de las actividades en la aplicación del Procedimiento GIC-PD-010-ACTUALIZACIONES O MODIFICACIONES DE COMPONENTES DE TECNOLOGÍAS DE INFORMACIÓN.</p>

	los productos de software, lo causa de lo anterior es la falta de aplicación de todas las actividades del procedimiento GIC-PD-010, lo cual genera debilidades en la documentación de los cambios realizados a los productos de software.(ejemplo definir estrategia de RollBack		
OBSERVACIÓN			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
2	<p>9. CONTROL DE ACCESO 9.4.5 Control de acceso al código fuente de los programas</p> <p>Se observa que se tienen un conjunto armonizado de elementos que permiten un control eficiente la gestión de acceso al código fuente y asegurar su confidencialidad, integridad y disponibilidad. Sin embargo se evidencia que las diferentes actuaciones para la implementación del control no está actualizado en la herramienta Agile</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	Adelantar las actividades necesarias para mantener las actuaciones de los controles actualizada en la herramienta Agile.
OBSERVACIÓN			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
3	<p>POLITICAS DE SEGURIDAD 5.1.2 Revisión de las políticas para la seguridad de la información.</p> <p>Se observa que se han realizado actualizaciones del documento políticas de seguridad por parte del jefe de la Oficina TIC de acuerdo con la delegación para el tratamiento de riesgos, sin embargo la revisión y aprobación de las Políticas de Seguridad no se realizó por parte del Comité CIDA durante la vigencia de 2017.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	Revisar los criterios y alcance de la delegación al jefe de la Oficina TIC para el tratamiento de riesgos del SGSI y asegurar que la actividad de realizar la revisión de las políticas tengan establecidos propietarios que ejerzan la responsabilidad del desarrollo, revisión y evaluación de las mismas y se permita la aprobación y la revisión por parte del Comité CIDA. Lo anterior con el fin de armonizar el control con la guía de implementación de la Norma ISO-27002

OPORTUNIDADES DE MEJORA			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
4	<p>INDICADOR DE LA EFECTIVIDAD DE LOS CONTROLES IMPLEMENTADOS EN EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN GIC-ID-008</p> <p>Se evidencia que el control está documentado y formalizado en el SGI. El oficial de seguridad informa que a la fecha no se han presentado incidentes de seguridad.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>El control está documentado y se está aplicando, la última medición registra 100%</p> <p>“No se tienen recomendaciones para este control”</p>
OPORTUNIDADES DE MEJORA			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
5	<p>14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.</p> <p>14.2.1 Política de desarrollo seguro Software.</p> <p>Se evidencia que el control está en proceso de implementación, a la fecha se ha avanzado en: GIC-FT-006 diligenciado para los Sistemas de Información desarrollados en la UPRA, en donde se incluyen los componentes de seguridad como los procesos de suministro de acceso y de autorización.</p> <p>En el formato GIC-FT-012 Documento de Arquitectura, en el capítulo de Atributos de Arquitectura se incluyen los drivers de negocio, en donde se registran los requisitos de seguridad de la información aplicables a los Sistemas de Información a desarrollar en la Unidad.</p> <p>Actualmente se encuentra en proceso de construcción la Guía Metodología de Referencia de Sistemas de Información, en la cual se incluyen las políticas de seguridad de la información aplicables a los Sistemas de Información a desarrollar en la Unidad. Se tiene planeado que esta</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Asegurar el plan de trabajo y recursos para finalizar y formalizar la implementación de las actuaciones de control y mantener actualizada la información de las actuaciones en el sistema Agile.</p>



INFORME FINAL DE AUDITORIA DE GESTIÓN



guía se formalice en el SIG para el mes de Julio de 2018.
Se evidencia que en la herramienta de Gestión del SGSI- Aggile los controles que están en estado cerrado no se pueden documentar y actualizar las actuaciones de implementación del control.

OPORTUNIDAD DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
6	<p>14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS</p> <p>14.1.1 Análisis y especificación de los requisitos de seguridad.</p> <p>Se evidencia que el control está en proceso de implementación, a la fecha se ha avanzado en: GIC-FT-006 diligenciado para los Sistemas de Información desarrollados en la UPRA, en donde se incluyen los componentes de seguridad como los procesos de suministro de acceso y de autorización.</p> <p>En el formato GIC-FT-012 Documento de Arquitectura, en el capítulo de Atributos de Arquitectura se incluyen los drivers de negocio, en donde se registran los requisitos de seguridad de la información aplicables a los Sistemas de Información a desarrollar en la Unidad.</p> <p>Actualmente se encuentra en proceso de construcción la Guía Metodología de Referencia de Sistemas de Información, en la cual se incluyen las políticas de seguridad de la información aplicables a los Sistemas de Información a desarrollar en la Unidad. Se tiene planeado que esta guía se formalice en el SIG para el mes de Julio de 2018</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Asegurar el plan de trabajo y recursos para finalizar y formalizar la implementación de las actuaciones de control y mantener actualizada la información de las actuaciones en el sistema Aggile</p>

OPORTUNIDADES DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
7	<p>INDICADOR DE LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI-GIC-ID-009</p> <p>Se evidencia que el indicador muestra avance en la implementación de los controles del SGSI basados en la normatividad, se concluye que el control está documentado y es eficiente.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Asegurar las actividades y recursos para cumplir con la implementación de los controles del SGSI de acuerdo con los plazos establecidos en la normatividad vigente. La última medición del indicador es del 110% lo cual indica un nivel de implementación de 88% a corte Diciembre de 2017.</p>

OPORTUNIDADES DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
8	<p>10. CIFRADO 10.1.1 POLITICA DE USO DE LOS CONTROLES CRIPTOGRAFICOS</p> <p>A la fecha no ha sido necesaria la aplicación de mecanismos de cifrado de acuerdo a la Guía de Clasificación y Rotulación de la Información, ya que se garantiza el acceso a la información únicamente al personal autorizado a través de la aplicación de permisos de acceso.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>No se presentan recomendaciones al control</p>

OPORTUNIDADES DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
9	<p>8. GESTIÓN DE ACTIVOS 8.1.2 Propiedad de los activos</p> <p>Se observa que se a pesar de que en las funciones de los cargos en general se idéntica funciones de cumplimiento con las directrices del Sistema Integrado de Gestión no se establecen funciones específicas con respecto a la seguridad de los activos de información que de los cuales son propietarios.</p> <p>Se observa que se han definido los propietarios de los activos de información en el inventario de activos de información, sin embargo se evidencia que no se ha establecido formalmente las responsabilidades de gestión sobre los activos de información, entre las cuales se puede nombrar: asegurarse que los activos estén inventarios, clasificados y protegidos apropiadamente, definir</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Evaluar alternativas para asegurar que las responsabilidades propias de los propietarios de activos de información sean ejercidas de forma efectiva. Lo anterior con el fin de armonizar el control con la guía de implementación de la Norma ISO-27002</p>

y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes teniendo en cuentas las políticas de control de acceso aplicables, asegurarse del manejo apropiado del activo cuando es eliminado o destruido. Lo anterior de acuerdo con el control 8.1.2

OPORTUNIDADES DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
10	<p>6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</p> <p>6.1.1 Roles y responsabilidades para la seguridad de la información.</p> <p>Se observa que se a pesar de que en las funciones de los cargos en general se identifican funciones de cumplimiento con las directrices del Sistema Integrado de Gestión no se establecen funciones específicas con respecto a la seguridad de los activos de información que de los cuales son propietarios.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Evaluar alternativas para asegurar que las responsabilidades propias de los propietarios de activos de información sean ejercidas de forma efectiva. Lo anterior con el fin de armonizar el control con la guía de implementación de la Norma ISO-27002</p>

OPORTUNIDAD DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
11	<p>13. SEGURIDAD EN LAS TELECOMUNICACIONES</p> <p>13.2.1 Políticas y procedimientos de intercambio de información.</p> <p>Se verificaron cinco (5) los formatos GI-FT-24-Gestión de insumos de información del periodo enero abril del 2018, se verifico la matriz de consolidación de requerimientos. Se evidencia que el control esta implementado y documento en el SGI mediante procedimientos y manuales debidamente controlados y diligenciados. Se tiene planeado salir producción con modulo en él SEA que automatiza el procedimiento GIC-PD-001 para el segundo semestre de 2018.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Asegurar el plan de trabajo y recursos para la automatización del Procedimiento GIC-PD-001 Gestión de insumos de información y suministro de productos UPRA</p>

OPORTUNIDAD DE MEJORA			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
12	<p>12. SEGURIDAD EN LA OPERATIVIDAD 12.1.2 Gestión de cambios</p> <p>Se evidencia que para los cambios de infraestructura generados por fallas en los componentes de Hardware de TIC no se aplica el procedimiento GIC-PD-010-ACTUALIZACIONES O MODIFICACIONES DE COMPONENTES DE TECNOLOGÍAS DE INFORMACIÓN, debido a que los cambios por mantenimiento correctivo se aplican a través del procedimiento GAD-PD-002 Mantenimiento preventivo y/o correctivo de bienes e infraestructura tecnológica del proceso Gestión Administrativa</p> <p>Se evidencia que los cambios a sistemas operativo no se aplica en procedimiento de Gestión de Cambios para esta situación se aplica el procedimiento Gestión de Servicios Tecnológicos GIC-PD-006</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>Se recomienda evaluar la pertinencia y eficacia de gestionar los cambios de la plataforma de tecnologías de información y las comunicaciones mediante diversos procedimientos y que pertenecen a dos procesos diferentes.</p>
OPORTUNIDAD DE MEJORA			
N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
13	<p>12. SEGURIDAD EN LA OPERATIVIDAD 12.3.1 Copias de Seguridad de la Información.</p> <p>Copias de seguridad de la información, no se presentan Hallazgos, observaciones u oportunidades de mejora</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	<p>No se tienen recomendaciones para este control</p>

OPORTUNIDAD DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
14	<p>16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.</p> <p>16.1.1 Responsabilidades y procedimientos.</p> <p>Se verifico la existencia de los formatos, procedimientos y guías y se revisó el consolidado de situaciones de seguridad, dichas situaciones se clasifican en eventos e incidentes, a la fecha no se tienen incidentes de seguridad y se han presentado 3 eventos. Se puede concluir que el control esta implementado, documentado y es eficiente.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	No se tienen recomendaciones.

OPORTUNIDAD DE MEJORA

N°	Descripción	Riesgo, Impacto, Categoría	Recomendación
15	<p>18. CUMPLIMIENTO</p> <p>18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.</p> <p>Se verificaron las actuaciones de la implementación y aplicación del control por lo que se puede concluir que el control esta implementado, documento y es eficaz, Adicionalmente se evidencia que las actuaciones no está actualizadas en el sistema Aggil.</p>	<p>Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA</p> <p>Menor Raro</p>	Asegurar las actividades y recursos para mantener actualizadas las actuaciones en el sistema Aggil

Anexos: No se tiene



Sandra Milena Ruano Reyes

ASESOR CONTROL INTERNO