INFORME DE AUDITORÍA

Código de auditoria: AUD-1668 Fecha: **Inicio** 2016-09-01 **Final** 2016-09-30

Fecha del informe: 2016-11-18

TIPO AUDITORIA	PROCESO, DEPENDENCIA O TEMA A AUDITAR	RESPONSABLE
Integral	Gestión Tecnológica y de la Información	LUZ MARCELA RAMIREZ VELEZ

OBJETIVO

Verificar la eficiencia, eficacia y efectividad en la implementación y administración de tecnologías de la información.

ALCANCE

Comprende la gestión adelantada durante el periodo Octubre de 2015 a Septiembre de 2016.

CRITERIOS

Normograma (leyes, decretos, resoluciones y acuerdos), caracterización y demás documentos del proceso publicado en el SIGER (procedimientos, instructivos, manuales, formatos y documentos externos), eficacia de los planes de mejoramiento finalizados, plan de acción y operativo, mapa de riesgos, Ley 1712 de 2014 de Transparencia y decretos reglamentarios.

AUDITOR LÍDER / DEPENDENCIA

JUAN CARLOS SEGURA PINZON

EQUIPO AUDITOR

ANA YANCY URBANO VELASCO

HALLAZGOS

1 Tipo Hallazgo: Oportunidad de mejora

Descripción: Se observó que los riesgos de TI son de carácter muy general para toda la función y que el cumplimiento de las medidas o acciones sobre su tratamiento tiene una periodicidad anual y en otros casos semestral, lo que no permite ejercer un monitoreo mas riguroso sobre la evolución del manejo de dichos riesgos.

2 Tipo Hallazgo: Oportunidad de mejora

Descripción: En el momento de nuestra revisión se evidencia que aunque se cuenta con un Datacenter externo, con muy buenas caracteristicas de seguridad y operación y está en etapa final de alistamiento y

		aseguramiento de un centro alterno de operaciones fuera de Bogotá, no se cuenta con un plan de continuidad de negocios para la ACR, (corresponde al denominado Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)), que incluya el impacto (BIA) desde el punto de vista de recursos humanos, físicos y financieros, debidamente documentado, actualizado y probado.
3	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se encuentran definidos como usuarios en producción, tres funcionarios desarrolladores que tienen privilegios de lectura y escritura sobre la base de datos de producción del aplicativo SIR. Estos usuarios son: Claudiaposada, Julianmadrid, Jerssonbetancourt
4	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se observó que no se tiene implementada la auditoria sobre las bases de datos.
5	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Para la instancia del aplicativo SIGOB se evidenció que para cada funcionario que va a ingresar en este aplicativo, se crea un usuario directamente en la base de datos.
6	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	En el momento de nuestra revisión se pudo comprobar que a pesar que se realizan actividades de la administración, monitoreo y mantenimiento de las bases de datos, no existen documentos formales sobre las políticas y procedimientos relacionadas con funciones realizadas por el funcionario encargado de ejecutar estas tareas.
7	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	De acuerdo a lo evidenciado actualmente no se cuenta con un mecanismo de cifrado de las bases de datos en su totalidad. Sin embargo se pudo establecer que si hay alguna información que se cifra, en particular cuando va dirigida a entidades externas.
8	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se realizó una comprobación en el módulo de seguridad del aplicativo SIR, en el cual se evidencia que existen los siguientes usuarios asignados al rol de administrador: CRM Implementador Production, Gloria Isabel Montoya Navarro, Jaime Eduardo Santafé Patino, Julian Andrés Madrid Caballero, Luis Alberto Duarte Moreno, Soporte SIR.
9	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se evidenció que la Entidad no dispone de políticas ni procedimientos documentados, dirigidos a administrar y monitorear en forma controlada y segura la creación, inactivación y eliminación de las cuentas de usuario registradas en los sistemas de información. Se identificaron funcionarios y contratistas que están retirados definitivamente o se encuentran en vacaciones, que están activos en el

Dominio de Windows Server 2012

10	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se observó que en el Directorio Activo se tiene como política de bloqueo = 0, lo anterior deriva en la posibilidad de poder realizar intentar accesos de forma ilimitada para ingresar a la red sin la autorización requerida.
11	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	En el momento de nuestra revisión se observó que tras las pruebas de penetración, existen 10 vulnerabilidades en progreso de remediación y 4 aún pendientes por resolver.
12	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se comprobó que existe un usuario en el área de seguimiento que ejecuta comandos SQL para la consulta de información de la base de datos de replica de SIR (ACRP_MSCRM) la cual esta en el nodo CETUS/DWH.
13	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	En la revisión del proceso de copias de seguridad, se observó que no se cuenta con un procedimiento formal para la restauración.
14	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	Se observó que no existen cronogramas ni manejo formal como proyecto para desarrollos de gran complejidad.
15	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	En los desarrollos y/o mantenimiento de software, se utilizan datos reales para las pruebas, lo cual dada la naturaleza de la agencia y el tipo de información (sensible) de la ACR, se puede ver afectada la confidencialidad de los datos.
16	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	No hay un Quality Assurance en el ciclo de vida del software.
17	Tipo Hallazgo:	Oportunidad de mejora
	Descripción:	En el procedimiento de desarrollo o modificación a programas, se utilizan usuarios finales en las pruebas del aplicativo en un ambiente similar al de producción, en el cual dichos usuarios finales, no se retiran posterior a las pruebas.

18	Tipo Hallazgo:	Oportunidad de mejora
Descripción:		No hay una aplicación de un modelo o metodología de gestión de proyectos tipo PMI.

19	Tipo Hallazgo:	Oportunidad de mejora
Descripción:		Se pudo establecer con el coordinador de sistemas de información de la OTI, que a pesar que la entidad ha establecido el acompañamiento de la OTI para cualquier aspectos que involucre adquisición de elementos tecnológicos, software, hardware o similares; desde las áreas usuarias, no siempre se solicita ese acompañamiento.

DESARROLLO

Durante la auditoría realizada al proceso de Gestión de Tecnología Informática - OTI, se desarrollaron los procedimientos descritos a continuación:

Entendimiento de la función de la OTI

Se efectuó un levantamiento del proceso de:

- Controles Gerenciales de la Función de la OTI en la ACR.
- Controles de Acceso a Sistemas y Bases de Datos.
- Controles para el Mantenimiento de los Sistemas de Información.
- Controles para las Operaciones de la OTI
- Controles para el Desarrollo de Proyectos

Los levantamientos de información cumplen con la práctica de auditoría de entender y evaluar controles, para posterior validar la efectividad de los controles asociados.

En particular para las pruebas de seguridad, se realizó una visita al Datacenter TIVIT - SYNAPSIS con una OLA (Operational Level Agreement) de esta compañía con EPM que es el proveedor de este servicio para la ACR, ubicado en la Zona Franca, en donde a través de observación, se pudo establecer que los controles asociados a la seguridad física, más que convenientes resultan muy adecuados para el aseguramiento de las áreas del Datacenter.

A nivel de controles de aplicación, se identificaron los siguientes:

- Controles de Acceso a las Aplicaciones.
- Controles de Validación en el Ingreso de Información.
- Controles para la Operación completa, exacta y oportuna de las aplicaciones.

En este caso, el entender y evaluar se cubre con una técnica de auditoría definida como el Walkthrough ó “ir a través de“, en este caso, el Software donde se fueron realizando pruebas de acceso y validaciones que permitían obtener una evidencia frente a los aspectos que se requerían evaluar.

OBSERVACIONES

N/A

RECOMENDACIONES

1. Fortalecer el soporte desde la OTI hacia los procesos de apoyo.
2. Se sugiere un control de las versiones no sólo con la versión en sí, sino con la fecha y hora de compilación del objeto ejecutable que se coloque en producción, incluso si la aplicación es tipo web, Aunque el versionamiento de SW se realiza por medio de la herramienta Team Foundatión.
3. Establecer una periodicidad real para la programación de las acciones sobre los riesgos de la OTI, con el fin de controlar y monitorear de forma oportuna las medidas adoptadas tendientes a mitigar los riesgos de tecnología informática.
4. Incluir en el plan estratégico institucional y con el apoyo de la Alta Dirección de la ACR, los programas y/o proyectos que involucre los procesos de apoyo y estratégicos, con una focalización complementaria a lo misional.
5. Desarrollar estrategias a nivel transversal, con la participación de las demás áreas de la entidad, que aseguren la implementación y puesta en marcha el SGSI para la ACR, lo cual deriva no sólo en el cumplimiento de los requisitos de GEL – Gobierno en Línea sino de aspectos normativos vigentes.
6. Realizar un proceso de depuración de las cuentas de usuarios en la Base de Datos SQL del SIR, en particular sobre los desarrolladores que tienen privilegios de escritura sobre la base de datos de producción de SIR.
7. Activar la auditoria (logs) sobre las bases de datos más relevantes, con el fin de realizar validaciones y seguimientos sobre las acciones realizadas por los usuarios, en el momento que así se requiera.
8. Solicitar al proveedor del aplicativo SIGOB que implemente una solución a la situación de crear usuarios en la base de datos por cada funcionario que ingresa al aplicativo, con el fin de mantener un mayor control sobre los usuarios y el acceso directo sobre la base de datos, ya que cualquier transacción se debe realizar directamente desde el programa SIGOB.
9. Diseñar, formalizar y divulgar políticas y procedimientos sobre la administración de las bases de datos, con el fin de gestionar el conocimiento y evitar se centralice en un funcionario que ejecuta las actividades inherentes a la administración de las bases de datos.
10. Evaluar si es aplicable el cifrado de las bases de datos, con el objetivo de fortalecer la seguridad de acceso a la información, lo cual mitigaría la perdida de datos en el caso de que se superen los controles de acceso.
11. Asignar solo dos administradores en el aplicativo SIR, esto con el fin de evitar acciones indebidas sobre la parametrización, inclusión, eliminación y modificación de la información relevante contenida en SIR de funcionarios no autorizados, además es necesario solicitar para el aplicativo SIR crear un rol para las funciones de implementador y soporte con el fin de separar estos perfiles del rol de administrador del programa.
12. Supervisar la rigurosa ejecución de las políticas y procedimientos (ya formalizadas) que aseguren un manejo seguro y controlado de las cuentas de usuario existentes, se debe involucrar a todas las áreas que tengan acceso a los sistemas de información lo que lo convierte en un tema a nivel transversal y que asegure entre otras acciones, la calidad de la información procesada a través de los sistemas de información, la completitud del registro de la misma y su integridad.
13. Implementar una política de bloqueo de la cuenta con mínimo 4 intentos fallidos, así como establecer el procedimiento o instructivo para el desbloqueo.
14. Implementar las soluciones pertinentes de las vulnerabilidades identificadas, 10 remediaciones en progreso y 4 pendientes. Lo anterior con el fin de garantizar una adecuada seguridad de la infraestructura de tecnología de la Entidad.
15. Revisar la conveniencia de contar con usuarios finales con acceso a la línea de comando en la base de datos de réplica de SIR.
16. Diseñar, implementar y aprobar un procedimiento de restauración de copias de seguridad, con una periodicidad

regular, con el fin de validar si estas copias se están generando de forma correcta y asegurar la integridad de la información contenida en ellas.

17. Diseñar cronogramas para los desarrollos de gran complejidad, con el fin de realizar un seguimiento efectivo sobre las actividades, recursos, riesgos y demás variables que tienen injerencia directa sobre los proyectos de nuevos requerimientos para el aplicativo SIR.
18. Se sugiere utilizar información real pero con un método que permita "anonimizar" la información aleatoriamente de ciertos campos, con el fin de que aun manejando datos reales en cuanto a estructura, no sea información exacta de los registros de la BD.
19. Implementar un modelo de aseguramiento de calidad en el desarrollo o ciclo de vida del software, con el fin de garantizar la calidad en el desarrollo de aplicaciones y nuevas funcionalidades de programas.
20. Establecer como parte de los procedimientos de cambios y/o desarrollo de software, en el capítulo relacionado con las pruebas y casos de uso con usuarios finales, sean retirados del ambiente de pruebas (desarrollo) dichos usuarios, después que se de el Vo. Bo. por parte de las áreas funcionales.
21. Evaluar la viabilidad de contar con una metodología formal de administración de proyectos, por ejemplo basado en PMI, que permitan asegurar el adecuado control de cada proyecto de complejidad importante para la entidad.

Finalmente, como resultado de esta auditoria se observaron algunos aspectos por mejorar que son transversales a toda la entidad. Las cuáles serán informadas en reunión con Dirección General, Secretaria General, Planeación para que se implementen las acciones a que hayan lugar:

- Se recomienda que la Dirección de la Entidad emita directrices y lineamientos a las diferentes dependencias para fortalecer la implementación del Sistema de Gestión de Seguridad de la Información en sus diferentes fases y etapas, en cumplimiento de la normatividad vigente.
- Adelantar las gestiones que se estimen pertinentes para, a nivel de la Entidad, incluyendo la función informática, diseñar, documentar, probar e implementar (en diferentes escenarios probables) un plan de continuidad de negocio (BCP) y de recuperación de desastres (DRP), que considere la adopción de medidas preventivas, detectivas y correctivas, orientadas a restaurar en forma oportuna y adecuada la materialización de un riesgo informático u operacional con medidas prácticas, viables y costeables.
- Reforzar desde la Alta Dirección que las áreas usuarias, soliciten a la OTI su acompañamiento, evaluación o concepto técnico y se convierta mandatorio que no se puede adquirir ningún tipo de elemento informático sin dicho concepto, este aspecto es a nivel transversal de todas las áreas que manejen herramientas de tecnología.

CONCLUSIONES

Realizada nuestra auditoría de la gestión de tecnología informática y de la Información en TI en la ACR, permite concluir que:

La entidad cuenta con un modelo de gestión de la Oficina de Tecnología Informática, con amplia orientación al cumplimiento del plan estratégico institucional, derivado a su vez del plan de gobierno y de una u otra forma respecto a lo establecido desde el DAPRE (Departamento Administrativo de la Presidencia de la República). Así mismo cuenta con un modelo de trabajo, muy orientado a la prestación de servicios de TI con filosofía de calidad, lo cual prevalece en una serie de ventajas que encaminan la OTI hacia un nivel de madurez suficiente respecto a las condiciones y necesidades de la misma Agencia.

El tener su infraestructura de TI fuera de las instalaciones administrativas de la ACR, es una buena práctica, así como contar con un sitio alterno fuera de la ciudad. Esto sin duda permite establecer un modelo de aseguramiento de la disponibilidad, más de lo esperado.

La OTI tiene claridad en el compromiso con el apoyo a la entidad, en particular a los procesos misionales, aspecto que se supone debería ampliarse a los demás procesos de la entidad.

Respecto a los temas de los aplicativos objeto de nuestra evaluación, es muy favorable contar con sistemas de información que permiten a las claras cumplir con los objetivos de cada área y particularmente con aspectos de gestión documental dado el hecho que se cuenta con sistemas de gestión que organizan de buena manera las operaciones a nivel transversal en la entidad.
Por otra parte en temas que resultan transversales a la entidad y por la naturaleza de la misma, la información sensible que aquí se maneja y el dinamismo que involucra a la ACR en el contexto nacional, es fundamental seguir trabajando en los proyectos que involucren los aspectos reglamentarios y de cumplimiento como son la Ley de Protección de Datos, Ley de Transparencia, pero particularmente los aspectos de Seguridad de la Información SGSI y los otros tres componentes de Gobierno en Línea, aspectos que se tienen en un buen porcentaje de cumplimiento pero que deben estar permanente monitoreado por todas las áreas involucradas.

Por último se requiere que se visualicen las recomendaciones emitidas como un fortalecimiento del ambiente de control interno de la OTI en la ACR. Aunque hay temas que deben generar planes de acción al corto plazo, no se pueden dejar de implementar, en particular temas relacionados con los accesos a las bases de datos, segregación de funciones, gestión del conocimiento, comprobación de la efectividad de las copias de respaldo, entre los más importantes.

ANEXOS

Anexo: Matriz Controles Generales TI - ACR Version Final.xlsx

Auditoria Interna de OTI V3 (002).docx