Informe de auditoría
Sistema de información SUIT

Distribuido a:

Roger Quirama García - Jefe Oficina de Tecnologías de la Información y las Comunicaciones

Diego Alejandro Beltrán - Director Gestión del Conocimiento (DGC)

Alejandro Becker Rojas - Director Desarrollo Organizacional (DDO)

Jaime Humberto Jimenez Vergel - Coordinador Grupo de Servicio al Ciudadano Institucional (GSCI)

Fernando Augusto Segura Restrepo - Director Dirección de Participación Transparencia y Servicio al Ciudadano "DPTSC"

Copias:

Liliana Caballero Duran – Directora General

Remitido por:

Luz Stella Patiño Jurado – Jefe Oficina Control Interno

Bogotá, 25 de Noviembre de 2017

Resumen ejecutivo auditoría al Sistema de Información SUIT

Objetivo:

Evaluar la efectividad de la gestión de riesgos y control tecnológico inmerso en la operación y administración del SUIT (Sistema Único de Información de Tramites), el cual es un instrumento de apoyo para la implementación de la política de racionalización de trámites que administra la Función Pública en virtud de la Ley 962 del 2005 y del decreto 019 del 2012. Además, de ser la fuente única y válida de información de los trámites que todas las instituciones del Estado ofrecen a la ciudadanía.

Es importante mencionar que las observaciones registradas en el presente informe coadyuvan a fortalecer el ambiente de control y seguridad del sistema de información actual.

Alcance:

La Auditoría será desarrollada desde la planificación de las actividades hasta la ejecución de las mismas, en el período comprendido entre el 10 de octubre de 2017 y el 30 de noviembre de 2017, a los siguientes ambientes:

- Producción:

  Para este ambiente se evaluarán los controles de Tecnología de la Información enfocados en los siguientes dominios:

  - Seguridad:

    - ✓ Gestión de acceso (Validación de usuarios y perfiles) y segregación de funciones.
    - ✓ Aseguramiento S.O. y B.D. (Verificación líneas base de seguridad - Hardening).
    - ✓ Controles de balanceo de integridad de la información entre componentes (Interfaces).

  - Operaciones:

    - ✓ Gestión de incidentes (Nivel 2 soporte funcional y técnico).
    - ✓ Procedimientos de contingencia.
    - ✓ Planes de continuidad.
    - ✓ Gestión de copias de respaldo y recuperación.

- Desarrollo (Versión 3):

    - Administración de cambios: Aprobación de la realización del cambio, documentación relacionada con el cambio en cada una de las etapas: análisis, desarrollo y pruebas (Funcionales – Técnicas), aprobación para el paso a producción y soporte técnico.

Procesos a auditar:

- Tecnologías de la Información (Oficina de Tecnologías de la Información y las Comunicaciones).
- Dirección de Participación Transparencia y Servicio al Ciudadano como Gestor de los procesos de Servicio al Ciudadano, Acción Integral en la Administración Pública Nacional y Territorial y Generación de productos y servicios para la gestión pública.

Lugar de ejecución de la auditoria: Instalaciones del Departamento Administrativo de la Función Pública pisos 2, 5 y 6.

Limitación en el alcance:

No se presentaron limitaciones en el alcance planeado.

Interpretación de los resultados de la auditoría:

Los aspectos evaluados en el proceso de auditoria tienen una interpretación según sus resultados, esta indica el grado de cumplimiento de los controles establecidos en el proceso o el impacto que supone la carencia o debilidad de los mismos. Algunos de los hallazgos son de responsabilidad directa del proceso y otros deben ser solucionados con el apoyo de las diferentes áreas objeto de la auditoría.

A continuación, se presentan las convenciones identifican la interpretación de los resultados:

Se aplica adecuadamente la normatividad vigente y los controles establecidos. No existen hallazgos sobre los asuntos evaluados.

La situación observada denota una debilidad que expone de manera indirecta o directamente a la entidad a un impacto negativo a nivel operativo o técnico, o un riesgo que se pueda materializar y requiere de una acción correctiva.

Riesgos evaluados

Riesgos Identificados en el proceso de auditoría	Cubierto en el alcance de la auditoría	Calificación de riesgo inherente según matriz de riesgos del proceso
Pérdida de confidencialidad e integridad de la información por accesos no autorizados, asociados con el ingreso a los sistemas de información, aplicativos, bases de datos o servidores sin autorización previa.	SI	Zona Alta
Pérdida en la disponibilidad o integridad de la información ocasionada por la afectación en la Infraestructura Tecnológica y servicios de TI como consecuencia de: - La no definición de la totalidad de los planes de continuidad de los servicios ofrecidos por TI. - Fallas o ausencia en la generación de copias de seguridad de los equipos servidores. - Falencias en los controles de las interfaces. - Fallas en niveles de mantenimiento y soporte.	SI	Zona Alta
Inadecuados servicios de soporte a incidentes o fallos tecnológicos, debido a: - Falencias en la definición o carencia de acuerdos de Niveles de Servicio (ANS) y/o de acuerdos de nivel operacional (OLA). - Capacidad operativa insuficiente. - Falta de conocimientos del personal. - Inadecuada clasificación de los incidentes reportados por parte de los usuarios.	SI	**No está identificado y evaluado en la matriz de gestión de riesgos de la Función Pública.**
Pérdida de imagen y riesgo legal debido a la ausencia o deficiencia en los registros, pistas o Logs de auditoria que permitan una investigación forense en la plataforma.	SI	**No está identificado y evaluado en la matriz de gestión de riesgos de Función Pública.**

Resultados aspectos evaluados

Detalle de las validaciones realizadas	Resultado	Item
Dominio Seguridad - Aseguramiento B.D: Aplicación de parches de seguridad actualizados, asignación de usuarios de operación, parametrización para recuperación de la información completa de la base de datos ante una falla del sistema, controles de acceso remoto y controles sobre modificación directa de datos en la B.D.		
Dominio Operaciones - Gestión de incidentes (Nivel 2 soporte funcional y técnico). Procedimientos de gestión y soportes, medición de la gestión.		
Dominio de operaciones gestión de cambios – procedimiento de sistemas de información, mantenimiento y desarrollo.		
Dominio Seguridad - gestión de acceso al sistema de información SUIT.		**H01**
Dominio Operaciones – Gestión de incidentes/requerimientos.		**H02**
Dominio Operaciones – Plan de continuidad SUIT		**H03**
Dominio Seguridad - Aseguramiento Bases de Datos (BD): Líneas base de seguridad.		**H04**
Dominio Operaciones – Gestión de copias de respaldo y recuperación.		**H05**

Hallazgos

H01: Inconsistencias usuarios activos en el sistema - Dominio Seguridad-Gestión de acceso al sistema de información SUIT.

Efectuando el cruce de información entre la base de usuarios internos matriculados en el sistema SUIT y en estado activo (44 usuarios), las plantas globales de personal y de contratistas, se evidencian los siguientes usuarios activos en el sistema, 2 de los cuales (Dos) ya están retirados y 2 (Dos) que cambiaron de rol y ya no deberían estar activos:

IDENTIFICACION USUARIO	NOMBRE_USUARIO	CUENTA USUARIO	ROLES	FECHA CREACION	HALLAZGO
40327912	LADY YADIRA VELASQUEZ	YVELASQUEZ	Asesor de política	03/11/2013	Cambio de rol este año
52086673	MARY WILCHES GARCÍA	MWILCHES673	Asesor de política Administrador de Plantillas y Modelos,	11/09/2015	Retirada desde septiembre de 2017
94372349	JOHNNY FABIAN TORRES APARICIO	JTORRES349	Asesor de política,	10/22/2013	Cambio de rol hace más de dos años
1056771448	MONICA YINETH DIAZ GARCIA	ADMINMIGRA1	Administrador de gestión,	02/28/2013	Creada temporalmente mientras la migración de versión del sistema, ya retirada.

Datos extraídos del Sistema de información SUIT con corte al 9 de noviembre de 2017

Riesgo(s) Evaluado Asociado a la Observación:

Pérdida de confidencialidad e integridad de la información por accesos no autorizados, asociados con el ingreso a los sistemas de información, aplicativos, bases de datos o servidores sin autorización previa.

Recomendación:

1.1. Previa verificación por parte del área responsable, se debe proceder a inactivar los usuarios inconsistentes mencionados en el hallazgo.

1.2 Mantener un estricto control y monitoreo del procedimiento de inactivación (retiro o cambio de rol) de funcionarios en el sistema de información SUIT. Es importante cumplir con el “Protocolo de seguridad y administración de usuarios y roles de SUIT” formalizado en el Sistema Integrado de Gestión del Departamento, en lo que respecta al procedimiento establecido para inactivación de usuarios.

H02: Ausencia de Acuerdos de Nivel Operacional "OLA" entre áreas responsables de soporte al SUIT - Dominio Operaciones – Gestión de incidentes.

Si bien se tienen definidos y parametrizados los ANS (Acuerdos de Nivel de Servicio) en la herramienta de mesa de servicio (Proactiva Net), donde se establecen los tiempos de atención para la gestión oportuna de incidentes y requerimientos por categoría a nivel funcional y/o técnico, a la fecha de evaluación no se tienen definidos OLA´s (Acuerdo de Nivel Operacional) internos entre las áreas de soporte (OTIC, DPTSC y GSCI).

Acorde con lo expresado por el Líder del Grupo de Servicios de Información de la OTIC (Oficina de Tecnología de la Información y las Comunicaciones), ya se tiene previsto a mediano plazo implementar una serie de OLA´s a nivel transversal entre los diferentes grupos de atención de soporte interno.

Riesgo(s) Evaluado Asociado a la Observación:

Inadecuados servicios de soporte a incidentes o fallos tecnológicos, debido a:

- Falencias en la definición o carencia de acuerdos de Niveles de Servicio (ANS) y/o de acuerdos de nivel operacional (OLA).
- Capacidad operativa insuficiente.
- Falta de conocimientos del personal.
  Inadecuada clasificación de los incidentes reportados por parte de los usuarios.

Recomendaciones:

Establecer Acuerdos de Nivel Operacional "OLA´s" internos, que determinen las relaciones técnicas y funcionales internas necesarias entre las áreas de soporte (OTIC, DPTSC y GSCI), y que sustenten los ANS establecidos, con el fin de establecer formal y claramente las responsabilidades de cada interviniente y la integralidad total de tiempos de solución que deben realmente conformar el tiempo total en cada ANS.

Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:

N/A – El Plan de Acción se emite posterior al informe.

H03: Falta de componentes fundamentales en el plan de continuidad del SUIT acorde con las mejores prácticas - Dominio Operaciones – Plan de continuidad.

Basados en las mejores prácticas soportadas por la norma ISO 22301:2012 para la Gestión de la Continuidad del Negocio. Esta auditoría evidenció los siguientes

aspectos susceptibles de mejora, que se consideran importantes para la minimización de los riesgos inherentes a la Continuidad del Negocio:

1. Si bien se evidencia la participación directa de la Dirección de Participación Transparencia y Servicio al Ciudadano - DPTSC como área misional, en las pruebas de continuidad no programadas realizadas a la fecha y coordinadas por la OTIC, dicha Dirección no ha sido incluida en las actividades del manejo de crisis en el documento del Plan de Continuidad del SUIT y tampoco ha sido sensibilizada al respecto.

2. Verificando el plan actual de continuidad y recuperación del servicio al sistema SUIT (Plan de Continuidad SUIT.docx) generado por la OTIC, se evidencia que aún está en proceso de construcción, por cuanto falta actualizar y/o completar:

   - El diagrama de flujo.
   - El procedimiento para Contingencia sin Sistema.
   - El Plan de Recuperación de Directorio Activo y de Plataforma de Virtualización.
   - Los posibles controles.
   - Los servidores responsables (Se encontró al servidor Gerson Enrique Carrillo con rol de administrador SUIT, quien a la fecha ya no ejerce este rol asignado).

3. No hay un informe que detalle los resultados de las pruebas relacionadas en la plataforma Proactivanet, efectuadas con la migración del nuevo servicio de nube privada y que van acordes con el Plan de Continuidad y Recuperación del Servicio para SUIT.

4. Los tiempos de ejecución de las actividades establecidos en el Plan actual, corresponden a tiempos con infraestructura interna, no se ha considerado el escenario con el proveedor de housing de nube privada, donde esta residente el ambiente de producción del sistema.

5. No se ha generado un cronograma de pruebas a futuro del Plan de Continuidad generado por la OTIC.

Riesgo(s) Evaluado Asociado a la Observación:

Pérdida en la disponibilidad o integridad de la información, ocasionada por la afectación en la Infraestructura Tecnológica y servicios de TI, como consecuencia de:

- La no definición de la totalidad de los planes de continuidad de los servicios ofrecidos por TI.
- Fallas o ausencia en la generación de copias de seguridad de los equipos servidores.

- Falencias en los controles de las interfaces.
- Fallas en niveles de mantenimiento y soporte.

Recomendaciones:

1. Incluir y sensibilizar a los Gestores de proceso de la DPTSC, que deban intervenir en el llamado a crisis dentro del Plan de Continuidad del Negocio del Sistema de Información SUIT, esto con el fin de considerar la transversalidad de todos los procesos que soportan tecnológica y operativamente la gestión de dicho Sistema.

2. Actualizar y/o completar el Plan de Continuidad y Recuperación del Servicio Sistema SUIT (Plan de Continuidad SUIT.docx), con los elementos evidenciados en el hallazgo.

3. Cuando se efectúen pruebas al Plan de Continuidad, sean o no programadas, es importante generar un informe con el detalle de las actividades efectuadas, sus gestores, tiempos de ejecución, desviaciones y conclusiones que permitan retroalimentar y mejorar el Plan existente.

4. Se hace necesario establecer los tiempos de las actividades de continuidad con el medio externo nube privada, teniendo en cuenta los ANS pactados a nivel contractual, e incluirlos en el Plan de Continuidad y Recuperación.

5. Elaborar una programación para la ejecución de pruebas periódicas al Plan de Continuidad implementado.

Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:

N/A – El Plan de Acción se emite posterior al informe.

H04: Ausencia de líneas base de seguridad para bases de datos Oracle - Dominio Seguridad - Aseguramiento B.D.

No se evidencian líneas base de seguridad (Hardening) para las bases de datos Oracle.

Durante la evaluación, por ejemplo, se encontraron aspectos relacionados con parámetros de contraseña para perfiles en la B.D. Oracle, donde se evidenciaron dos (2) tipos de perfiles “DEFAULT” y “MONITORING_PROFILE", con parámetros de contraseña diferentes (Parámetros: CONNECT_TIME, IDLE_TIME, SESSIONS_PER_USER, FAILED_LOGIN_ATTEMPTS, PASSWORD _GRACE_TIME, PASSWORD_LIFE_TIME, PASSWORD_LOCK_TIME, PASSWORD_REUSE_MAX, PASSWORD_REUSE_TIME, PASSWORD_VERIFY_FUNCTION). Esta configuración no se encuentra soportada por una línea base de seguridad.

A pesar que los parámetros de configuración de seguridad de la B.D. están bajo las mejores prácticas recomendadas (Accesos de rol público, propietarios de tablas de usuario final, accesos remotos sin autenticación, segregación de usuario con altos privilegios, entre otros), no se evidencia una línea base de seguridad que soporte esta configuración y que asegure su grado de actualización en los sistemas y su monitoreo periódico.

Riesgo(s) Evaluado Asociado a la Observación:

Pérdida en la disponibilidad de la información, ocasionada por la afectación de la infraestructura tecnológica como consecuencia de: Manipulación inadecuada en la infraestructura, fallas u obsolescencias de elementos que componen la infraestructura tecnológica, parametrización errada de seguridad y soporte.

Recomendaciones:

Establecer mejoras en el dominio de gestión de la configuración de seguridad en los sistemas del DAFP, mediante la implementación de líneas base de seguridad que permitan preparar los sistemas informáticos y las aplicaciones para resistir de forma adecuada ciberataques conocidos y desconocidos, que aprovechan vulnerabilidades para ser cometidos. Específicamente para los elementos que componen el sistema de información SUIT (S.O., B.D., Servidores, entre otros).

Las líneas base de seguridad deben contener como mínimo:

- Procedimientos de actualización de versiones para S.O. y B.D.
- Configuraciones de seguridad necesarias para protegerse de posibles ataques cibernéticos, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.
- Instalación, configuración y mantenimiento de programas de seguridad tales como: Antivirus, Antispyware y un filtro Antispam según las necesidades del sistema.
- Configuraciones de seguridad orientadas a gestión de usuarios, de políticas de contraseña robusta (Claves caducables, almacenamiento histórico de contraseñas, bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseña), renombramiento y posterior deshabilitación de cuentas estándar del sistema, como administrador e invitado, asignación correcta de derechos de usuario, de tal manera que se reduzcan las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los mismos y/o derechos de los usuarios activos.
- Restricciones de software, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo (Licenciamiento).
- Activación de auditorías del sistema; teniendo en cuenta el rendimiento de las máquinas y el consumo de recursos.

- Configuración de servicios de sistema. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema.
- Configuración de acceso remoto. Restricciones de acceso a un número muy limitado de usuarios y al mínimo las conexiones concurrentes, teniendo cuidado en la desconexión y cierre de sesión y el establecimiento de un canal cifrado de comunicaciones para tales propósitos, como SSH, por ejemplo.
- Configuración adecuada de cuentas de usuario, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de usuarios, para realizar labores administrativas en vez de iniciar sesión como administradores.

Una vez implementadas estas líneas base en el entorno informático, es fundamental que la Entidad establezca procedimientos de control, que permitan medir si estas líneas base de seguridad siguen cumpliendo con su objetivo primordial, ejecutando estudios de análisis de vulnerabilidades, los cuales alimentan tanto el proceso de remediación como el proceso de fortalecimiento y la actualización de dichas líneas.

Plan de acción definido por el responsable / Responsable / Fecha de cumplimiento:

N/A – El Plan de acción se emite posterior al informe.

H05 – Ausencia de planes de restauración y ejecución de pruebas de respaldos de la Base de Datos del Sistema de Información. Dominio Operaciones – Gestión de copias de respaldo y recuperación.

Actualmente el procedimiento de toma de copias de respaldo a nivel interno y externo para el Sistema SUIT se efectúa de manera correcta, no obstante, no se evidencia un plan de pruebas de restauración de las copias de respaldo tomadas periódicamente y enviadas a medio externo, las cuales están soportadas bajo los procedimientos propios de las Políticas de Respaldo, Custodia y Recuperación de la Información establecidas formalmente.

Riesgo(s) Evaluado Asociado a la Observación:

Pérdida en la disponibilidad o integridad de la información, ocasionada por la afectación en la Infraestructura Tecnológica y servicios de TI como consecuencia de:

- La no definición de la totalidad de los Planes de Continuidad de los Servicios ofrecidos por TI.
- Fallas o ausencia en la generación de copias de seguridad de los equipos servidores.
- Falencias en los controles de las interfaces.
- Fallas en niveles de mantenimiento y soporte.

Recomendación:

Implementar un plan de pruebas de restauración permanente y periódico de las cintas de respaldo enviadas a medio externo, bajo los procedimientos descritos en las políticas de respaldo, custodia y recuperación de la Información del DAFP. Permitiendo así garantizar que las tecnologías y procedimientos son exitosos en cuestión de respaldo de información y así mismo, medir la eficacia en la restauración de la información ante eventos de fallo que atenten contra la disponibilidad del sistema. Parte del plan está en mantener los soportes e informes correspondientes a cada prueba.

Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:

N/A – El Plan de Acción se emite posterior al informe.

Luz Stella Patiño Jurado
Jefe Oficina Control Interno

Elaboró: Ingeniero Juan Mauricio Cornejo Rodríguez