Función Pública

Informe de auditoría sistema SUIT

Evaluación Independiente

Función Pública

Informe de auditoría sistema SUIT

Sistema de información SUIT

Informe Detallado: John Ricardo Morales Franco- Jefe de Oficina de Tecnologías de la Información y las Comunicaciones

Aura Isabel Mora– directora de Transparencia, Participación y Servicio al Ciudadano

Milena del Rocío Trujillo Chaparro – jefe(e) Oficina OREC

Alveiro Tapias Sánchez – jefe Oficina Asesora de Planeación

Resumen Ejecutivo: Cesar Augusto Manrique Soacha - Director General
Miembros del Comité Directivo

Emitido por: Jorge Iván De Castro Barón - jefe Oficina de Control Interno

23 DE JULIO 2024

Resumen Ejecutivo

Auditoría con Enfoque Basado en Riesgos al Sistema de Información SUIT

Objetivo:

Evaluar la efectividad de la gestión de riesgos y control tecnológico inmerso en la operación y administración del sistema de información SUIT (Sistema Único de Información de Trámites), el cual, es la herramienta utilizada como única fuente válida de la información de todos los trámites y otros procedimientos administrativos que realizan los ciudadanos, empresarios, inversionistas y servidores públicos frente a las entidades de la administración pública colombiana, como insumo para simplificar, estandarizar, eliminar, optimizar y automatizar trámites y otros procedimientos administrativos OPA, acorde con la política de racionalización de trámites del Modelo Integrado de Planeación y Gestión (Decreto 1083 de 2015), Ley 962 de 2005, el Decreto Ley 019 de 2012 y la Resolución 1099 de 2017.

Alcance:

La auditoría se llevará a cabo de manera presencial y virtual, mediante el uso de la herramienta Microsoft Teams para las entrevistas; para la revisión documental se consultará el servidor de carpetas compartidas “Yaksa”, el Sistema Integrado de Planeación y Gestión (SIPG) y el Sistema de Gestión Institucional (SGI). El periodo de evaluación comprende la vigencia 2023 y del 1° de enero al 30 de abril de 2024. Las evaluaciones se realizarán, teniendo en cuenta los siguientes escenarios:

- Gestión Contractual:

  - ✓ Ejecución contractual - Contrato interadministrativo 042/2024 CORPORACION AGENCIA NACIONAL DE GOBIERNO DIGITAL- soporte BD para el sistema SUIT.

- Controles generales de TI (Capa de Aplicación):

  - ✓ Gestión de acceso lógico a la aplicación (Administración usuarios, parámetros de contraseña)
  - ✓ Monitorización de actividad crítica – logs
  - ✓ Respaldo y recuperación de la información
  - ✓ Gestión de Seguridad de la información (Controles de aseguramiento)
  - ✓ Gestión de incidencias (Controles cumplimiento ANS - OLAs)
  - ✓ Gestión del cambio (Mejoras o nuevos desarrollos)
  - ✓ Continuidad de negocio
  - ✓ Interoperabilidad

Además, de lo establecido en los siguientes documentos:

- ✓ Manual de Contratación Proceso de Gestión de Recursos – Subproceso de Gestión Contractual. v16/2022.
- ✓ Guía para gestionar incidencias y requerimientos del Sistema -SUIT. V2/2029.
- ✓ Contrato interadministrativo 042/2024 AND.
- ✓ Instructivo Administración de las Bases de Datos. V2/2019
- ✓ Lineamientos para la Gestión de Cambios de Tecnologías de la Información. V1/2020.
- ✓ Protocolo de Seguridad, Administración de Usuarios y Roles SUIT. V6/2023
- ✓ Plan de Seguridad y privacidad de la información. V1/2023.
- ✓ Plan de recuperación ante desastres tecnológicos - Proceso de Tecnologías de la Información. V1/2022.
- ✓ Plan de continuidad y recuperación para el aplicativo SUIT - Proceso de Tecnologías de la Información. V2/2022.
- ✓ Política de Operación proceso de Tecnologías de la Información. v8/2021.
- ✓ Políticas Técnicas de Seguridad de la Información - Proceso de Tecnologías de la Información. v6/2023.
- ✓ Política de respaldo, custodia y recuperación de la información - Proceso de Tecnologías de la Información. v5/2023.
- ✓ Documento Técnico del Plan de Continuidad del Negocio. V5/2023
- ✓ Manual Metodología de Riesgos. V7/2022
- ✓ Mapa de Riesgos Institucional 2024. v27/2024
- ✓ Plan Estratégico de Continuidad del Negocio. v1/2024
- ✓ Riesgos e Indicadores del proceso SGI.

Metodología:

Cada etapa de la auditoría interna con enfoque basado en riesgos (entendimiento del proceso, evaluación del riesgo, pruebas de recorrido y de validación de controles), será desarrollada así:

- ✓ Lectura y revisión de la documentación vigente.
- ✓ Entrevistas con los funcionarios que intervienen en la gestión técnico-operativa de la administración del sistema y de la supervisión del convenio interadministrativo 042/2024.
- ✓ Análisis de la información requerida para el desarrollo de la auditoría.
- ✓ Inspección de documentos relacionados con la ejecución de la auditoria.
- ✓ Pruebas de recorrido y de efectividad de controles físicas y/o virtuales.

Limitaciones de la Auditoría:

Interpretación de los resultados de la Auditoría: Los aspectos evaluados en el proceso de auditoría interna tienen la siguiente interpretación según sus resultados, indicando el grado de cumplimiento de los controles establecidos en los riesgos evaluados o el impacto que supone la carencia, debilidad o recurrencia de éstos.

	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 un riesgo que se pueda materializar y requiere de una acción correctiva.
(R)	Hallazgo Recurrente. Observado en seguimientos y auditorías anteriores internas y/o externas, el cual se presentará al Comité Institucional de Coordinación de Control Interno para el establecimiento de lineamientos en las acciones de mejora a implementar.

Resultados del Trabajo

Riesgos y Aspectos Evaluados

Riesgos identificados en el proceso de la auditoria	Calificación del riesgo inherente según matriz de riesgos del proceso	Cubierto el alcance de la auditoria	Detalle de las validaciones realizadas	Resultado	No. De hallazgo (ver Informe Detallado)
1. Posibilidad de pérdida económica y/o reputacional por Incumplimiento a las obligaciones específicas y generales definidas en el contrato interadministrativo, debido a fallas en la supervisión del mismo o en la inconcreción de las obligaciones.	No incluido en la matriz de riesgos.	SI	Adecuada gestión de control y vigilancia sobre la ejecución contractual.		H 1.1
2. Posibilidad de pérdida reputacional por divulgación no autorizada de información reservada o clasificada almacenada en los repositorios institucionales o sistemas de información debido a la inadecuada gestión de los permisos de acceso. (DPTSC)	BAJA	SI	Apropiados controles de asignación de usuarios operativos y segregación de funciones para el acceso al sistema.		H 2.1

3. Posibilidad de pérdida reputacional por queja, demanda o sanción de los grupos de valor y/o entes de control debido a pérdida de confidencialidad en activos que contiene información con carácter personal administrados por la OTIC	ALTA	SI	Adecuados procedimientos técnicos y operativos de administración de usuarios y roles en el sistema, registro de operaciones y controles de interoperabilidad con el fin de prevenir accesos no autorizados.		H 3.1
4. Posibilidad de pérdida reputacional por quejas y sanciones de entes de control debido a pérdida de disponibilidad o incumplimiento de los ANS (acuerdos de niveles de servicio) de los servicios y sistemas de información administrados por la OTIC, causados por incidentes de seguridad fuera de control	ALTA	SI	Apropiado procedimiento de gestión de incidentes de la plataforma.		H 4.1
			Aspectos susceptibles de mejora en la definición de los planes de contingencia técnico y operacionales del SUIT.		H 4.2
5. Posibilidad de pérdida reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de Integridad (modificación no autorizada) de la información o configuración de los servicios	ALTA	SI	Adecuados controles y procedimientos para la gestión de cambios en el sistema.		H 5.1
			Apropiados controles y procedimientos para respaldo y recuperación de la información manejada por el sistema.		H 5.2

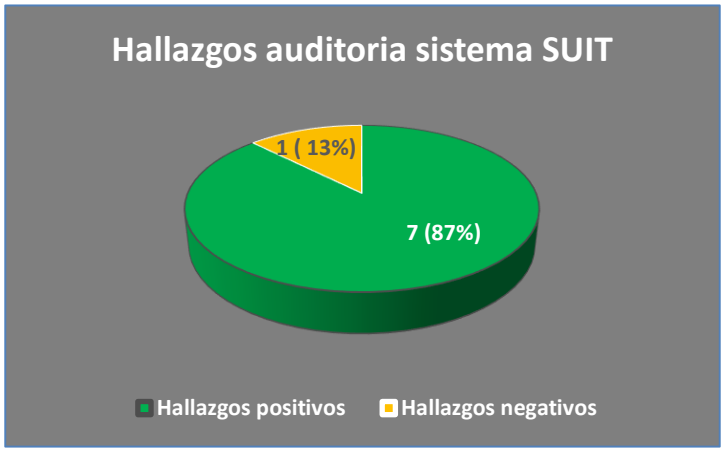
gestionados por la OTIC causados por posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falla tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware					
			Adecuados controles y procedimientos de seguridad de la información.		H 5.3
Hallazgos: Ver el informe Detallado- Ruta en Yaksa: \\yaksa.dafp.local\10010OCI\2024\DOCUMENTOS_APOYO\PROGRAMAS\PROGRAMAS_AUDITORIA_INTERNA\AUDITORIA_SUIT\3_RESULTADOS					

Conclusiones y Recomendaciones Generales

1. Se destaca la disposición y colaboración brindada por parte de los servidores de la Oficina de Tecnologías de la Información y las Comunicaciones que administran tecnológicamente el sistema, así como a la Dirección de Transparencia, Participación y Servicio al Ciudadano que intervienen en la gestión administrativa y operativa del sistema SUIT, lo cual permitió que, a través de entrevistas y aporte de información, se pudiera verificar la efectividad de los controles establecidos por parte del proceso.

2. Se denota el volumen y la calidad de la información suministrada al usuario a través de políticas, manuales y guías implementadas en el micrositio de SUIT y en el SIGP.

3. En la auditoria efectuada al sistema SUIT, se definieron ocho (8) hallazgos, de los cuales en siete (7) hallazgos (87%), se pudo evidenciar una aplicación adecuada de la normatividad vigente y los controles establecidos acorde con las mejores prácticas; así mismo, se evidenció un (1) hallazgo (13%), en el que se observa situaciones que denotan una debilidad que expone de manera indirecta o directamente a la Entidad a un impacto negativo a nivel operativo o un riesgo que se pueda materializar y requiere de una acción correctiva. Por lo anterior, se hace necesario hacer seguimiento a las desviaciones de la gestión comunicada y emprender las acciones de mejoramiento continuo, a través del Sistema de Gestión Institucional – SGI.



4. Bajo el esquema plan de continuidad de negocio de la entidad y con el apoyo de la OAP, Involucrar en la estrategia de solución de continuidad para el SUIT, a la Dirección de Participación, Transparencia y Servicio al Ciudadano - DPTSC.

5. Es necesario revisar la pertinencia de incluir en la matriz de riesgos institucional, el riesgo

identificado por la Oficina de Control Interno en la presente Auditoría Interna de Gestión con Enfoque Basado en Riesgos, definidos en el informe ejecutivo como “Riesgo no incluido en la matriz de riesgos del proceso”.

Plan de Mejoramiento Institucional

Plan de acción definido por el responsable / Responsable / Fecha de cumplimiento: El Plan de Mejoramiento Institucional es la herramienta que permite consolidar y evidenciar los diferentes hallazgos, las oportunidades de mejora, el seguimiento a las desviaciones de la gestión y las acciones de mejoramiento continuo emprendidas en la Entidad, a través del Sistema de Gestión Institucional - SGI. Con el fin de incluir las acciones para subsanar los hallazgos de la presente auditoria, se llevará a cabo el procedimiento establecido en el “Manual del Usuario SGI - Módulo Plan de Mejoramiento”

Jorge Iván De Castro Barón
Jefe de Control Interno

Elaboró: Juan Mauricio Cornejo R. - Contratista Oficina de Control Interno
Revisó y aprobó: Jorge Iván de Castro Barón - Jefe Oficina Control Interno

Función Pública

Informe de auditoría sistema SUIT

Proceso Tecnologías de la Información

Julio de 2024

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 12 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)