SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

INFORME AUDITORIA BÁSICA SISTEMA INTEGRAL DE CAPTURA DE LA SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA -SICSES

OFICINA DE CONTROL INTERNO

Septiembre de 2019

Tabla de contenido

1. GENERALIDADES DEL INFORME 3
1.1 INTRODUCCION. 3
1.2 OBJETIVO GENERAL 3
1.3 OBJETIVOS ESPECIFICOS 3
1.4 ALCANCE 4
1.5. METODOLOGIA 4
2. RESULTADOS DEL INFORME 4
3. OBSERVACIONES Y RECOMENDACIONES 11

1. GENERALIDADES DEL INFORME

1.1 INTRODUCCION.

De conformidad con lo establecido en el artículo 9° de la Ley 87 de 1993 le corresponde a la Oficina de Control Interno, asesorar a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos, en desarrollo de tales funciones, el artículo 17 del Decreto 648 de 2017, identifica la evaluación y seguimiento, como uno de los principales tópicos que enmarcan el rol de las Oficinas de Control Interno.

De igual forma, y teniendo en cuenta que el artículo 6º del Decreto 648 de 2017, establece que le corresponde a la Oficina de Control Interno en cada entidad "Medir y evaluar la eficiencia, eficacia y economía de los demás controles adoptados por la entidad, así como asesorar y apoyar a los directivos en el desarrollo y mejoramiento del Sistema Institucional de Control Interno a través del cumplimiento de los roles establecidos", mediante la formulación de recomendaciones y observaciones para lograr el cumplimiento de las funciones y objetivos misionales, dando cumplimiento a lo dispuesto en el Programa Anual de Auditoria para la vigencia del año 2019, en su componente de auditorías especiales, en su actividad No. 21 – Auditoria Básica Aplicativo SICSES, la Oficina de Control Interno presenta el informe de la auditoria básica al Sistema Integral de Captura de la Superintendencia de la Economía Solidaria - SICSES.

1.2 OBJETIVO GENERAL

Verificar el estado de operación del sistema desde el ingreso de información hasta que la información queda disponible para que se usada por los funcionarios de la Superintendencia en los aplicativos"Fabrica de reportes y BI inteligencia de negocios".

1.3 OBJETIVOS ESPECIFICOS

- Revisión del proceso de liberación de versiones.
- Revisión del proceso de control de cambios.
- Evaluación de los manuales técnicos y de usuario.
- Análisis de controles de la información a nivel de acceso y salvaguarda de la misma.
- Análisis de la plataforma tecnológica que soporta el sistema.

1.4 ALCANCE

Se evaluó la gestión alrededor del procedimiento de liberación de versiones y la metodología usada para la gestión de los cambios en el mes de junio de 2019.

1.5. METODOLOGIA

- La Oficina de Control Interno solicitó a la Oficina Asesora de Planeación y Sistemas una relación con la información detallada relacionada con el sistema

- Se realizaron entrevistas con el desarrollador, con el encargado del centro de cómputo, con el contratista de la base de datos y con el líder de los sistemas

- Cada entrevista se realizó en aproximadamente una hora y los temas tratados estaban relacionados directamente con las funciones realizadas asociadas al sistema de información SICSES.

- Se realizó análisis y lectura de la información recolectada, interrelacionándola y revisando la aplicación de buenas prácticas como ITIL e ISO y directrices de MinTIC.

- Se analizó el procedimiento utilizado para el control de cambios y la implementación de versiones ajustadas del sistema de información SICSES.

Referencia: Guía para la preparación de las TIC para la continuidad del negocio: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

Plan de Continuidad de Negocio. Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción. NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301]

2. RESULTADOS DEL INFORME

De la revisión y análisis de los archivos y aplicando la metodología indicada se encontraron los siguientes resultados:

2.1 El plan de continuidad del negocio entregado a la Oficina de Control Interno no está actualizado y data del año 2014.

a. No se realizan pruebas de ejecución del Plan de Continuidad del Negocio desde hace cuatro años y medio, luego la viabilidad de éxito de la aplicación del Plan no está comprobada y asegurada para el escenario y estado de arte de TI del año 2019, donde actualmente tenemos servidores de hiperconvergencia y sistemas de seguridad de las comunicaciones Fortinet versión reciente la cual fue implementada en el 2019.

b. En la matriz de riesgo incluida en el Plan de Continuidad del Negocio, relacionan tres (3) riesgos de los cuales, solo uno está relacionado con el Plan de continuidad "*interrupción total o parcial de los servicios que componen la plataforma tecnológica de la entidad*".

   En la misma matriz de riesgo no están incluidos eventos de tipo catastrófico donde no solo las operaciones de tecnología se vean suspendidas; de igual forma no se contemplan eventos como pérdida de la sede por terremoto.

c. El Plan de Continuidad del Negocio no define completamente el punto de recuperación (RPO por su sigla en inglés para Recovery Point Objetive), se limita a indicar en tiempo cuanto se demora en recuperar cada servicio desde el punto de vista tecnológico y no contempla a las personas, espacios de trabajo y cuáles serían las condiciones de trabajo.

d. El Plan de Continuidad del Negocio entregado para verificación no presenta información relacionada con:

   - Sitio alterno de procesamiento
   - Sitio alterno de trabajo fuera de la sede actual
   - Esquema o estrategia de prueba periódica del Plan de Continuidad del Negocio.
   - No presenta la estrategia de actualización de la información del sitio alterno de procesamiento de datos.
   - Presupuesto y costo de cada una de los ítem relacionados con el Plan de Continuidad del Negocio.
   - Estrategia de información y comunicación a los funcionarios, contratistas, Clientes y al Ciudadano relacionados con la implementación y uso de los sitios de atención.

2.2. De la lectura y análisis del INSTRUCTIVO REPORTE DEL FORMULARIO OFICIAL DE RENDICIÓN DE CUENTAS - SICSES, identificado como D-GEIN-010, considerado como el manual del usuario presentamos a consideración las siguientes observaciones:

a. Es un documento de 306 páginas, el cual tiene un índice con las páginas donde se encuentra cada tema, pero el documento no está paginado.

b. Como es un documento para uso de los entes vigilados, este es no tiene una guía especifica donde cada tipo de ente tenga una paquete de formatos asociados. El manual presenta todos los formatos haciendo difícil el uso y la comprensión.

c. No parte de lo general a lo particular, esto quiere decir relación de entes vigilados, para que el usuario se ubique cual es el suyo y posteriormente se indique que formatos debe diligenciar, cuales son obligatorios y cuales son opcionales y ahí si iniciar con la descripción y uso de cada uno.

d. No tiene un capítulo de preguntas y respuestas frecuentes.

e. Dentro de cada formato no describe los posibles errores y la correspondiente solución para facilitar la corrección de información.

2.3. Revisando el flujograma del proceso de cambios y atención a requerimientos entregado como documento guía de la Oficina Asesora de Planeación y Sistemas observamos:

a. De acuerdo con las buenas prácticas de desarrollo de software (Rational Unified Process RUP y Scrum) en la gráfica existe el proceso de desarrollo de la Oficina Asesora de Planeación y sistemas, después del análisis de la viabilidad del requerimiento, el ciclo de vida de desarrollo de software requiere la etapa de análisis y diseño, esta etapa se realiza por un arquitecto de software y debería ejecutarse una vez termina la etapa de especificaciones y antes del desarrollo o codificación. La etapa de análisis y diseño que ejecuta un arquitecto de sistemas no se visualiza en el diagrama.

b. De acuerdo con las entrevistas y la revisión del procedimiento de control de cambios por parte de la Oficina Asesora de Planeación y Sistemas no existe un ambiente de desarrollo, ubicado en el centro de datos y controlado por procesamiento, en la actualidad esta tarea se realiza en cada uno de las estaciones de trabajo de los desarrolladores. Al final del desarrollo se actualiza el SVN (sistema de control de fuentes y despliegues) y se realizan copias de seguridad. Las buenas prácticas como ITIL requieren la existencia del ambiente de desarrollo.

c. De acuerdo con las entrevistas y la revisión del procedimiento de control de cambios por parte de la Oficina Asesora de Planeación y Sistemas no existe un ambiente de pruebas, ubicado en el centro de datos y controlado por procesamiento, en la actualidad esta tarea se realiza en cada una de las estaciones de trabajo con datos reales y en ocasiones en el ambiente productivo.

2.4. De la lectura, análisis y evaluación del documento POLITICAS DE GENERACION DE BACKUPS DE LA ENTIDAD, observamos:

a. No están definidos los riesgos por cada sistema de información o base de datos donde se establezca el tiempo que trascurre entre cada copia de seguridad y como este tiempo de actualización de información y adición de registros se va a mitigar.

b. La política tiene fecha de octubre del 2018, pero no se evidencia su publicación, apropiación y uso de la misma, no tiene identificador documental, ej. D-GEIN-010

c. Dentro del documento mencionado en el capítulo 4 numeral 4.1.1 indica: "*El área de planeación y sistemas debe determinar al menos una vez al año las necesidades de recuperación. Ello consiste en identificar la necesidad de contar con copias de respaldo de procesos, aplicativos y datos*", no se encontró evidencia anual de las necesidades de recuperación.

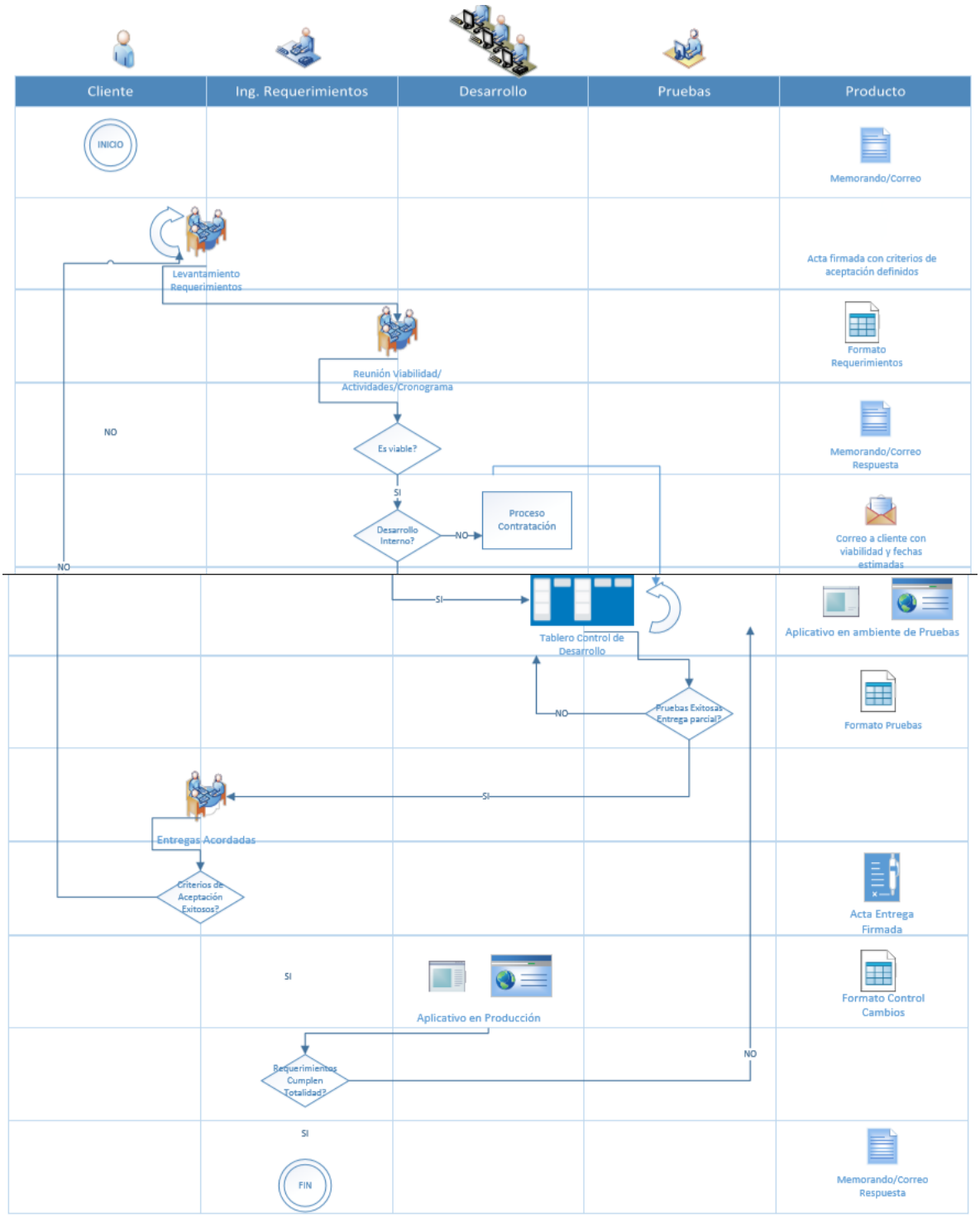
d. Se mezcla el concepto de política con el de procedimiento, esto se evidencia en el capítulo "*Administración de copias de respaldo* ", el numeral 4.3.3 dice: "*Los dispositivos que contienen las copias de respaldo serán guardados en el centro de cómputo bajo llave y en custodia del administrador del área de sistemas*".

2.5. De la lectura, análisis y evaluación del documento R-GEIN-009 Realizar copias de respaldo a la base de datos de junio 26 del 2015 encontramos:

a. El documento presenta desactualización de cuatro años.

b. No contempla la prueba de aseguramiento de la copia de seguridad, esto se realiza efectuando la restauración de la misma y comprobando su consistencia e integridad en la descarga, de acuerdo como lo indica en la Política entregada en el capítulo 4.2 Respaldo de la información numeral 4.2.3 "*Se llevará un registro de las pruebas de recuperación de las copias de resguardo, con la finalidad de constatar que se pueden recuperar correctamente los datos grabados en el medio magnético al momento de ser necesarios*".

2.6. De la lectura, análisis y evaluación del documento **"**procedimiento de desarrollo", se observa:



Carrera 7 No. 31-10 Piso 11. PBX (1) 7 560 557. Línea Gratuita 018000 180 430
www.supersolidaria.gov.co
NIT: 830.053.043 5 Bogotá D.C., Colombia

a. No están resueltas o claras las rutas del flujo a seguir para:
   - Si los criterios de aceptación son aprobados
   - El momento en que se pasa a producción
   - Cuando los requerimientos no cumplen
   - Cuando los requerimientos de aceptación no son aprobados

b. El flujo muestra que pasa a levantamiento de requerimientos cuando los criterios de aceptación del requerimiento no son aprobados, este paso debe devolverse a desarrollo para el ajuste y no volver a revisar las especificaciones.

2.7. Del análisis de la tabla de usuarios con 1.410 registros asignando derechos a la base de datos encontramos:

a. La base de datos registra 6 usuarios así:

USUARIO	DERECHO	RECURSO / OBJETO	OBSERVACION
ANONYMOUS	Executar	CONSULTA_ENTIDADREG	Viene por defecto
CONSULTA	Executar	varios	Solo de consulta
	Select	varios	Solo de consulta
CONSULTASGD	Select	SELECT	Gestión documental
SUI3	ALTER	Tablas de datos en producción, funciones (procedimientos o rutinas), validaciones y formatos de resultado	Usuario de alto riesgo, todos los de sistemas lo usan, tiene la misma clave, tiene 619 asignaciones de derechos sobre los recursos de información de la base de datos
	EXECUTE		
	DEBUG		
	DELETE		
	INDEX		
	INSERT		
	UPDATE		
	REFERENCES		
	ON COMMIT REFRESH		
	QUERY REWRITE		
	FLASHBACK		
	EXECUTE		
SUI5	Select	Tablas de datos en producción, funciones (procedimientos o rutinas), validaciones y formatos de resultado	Usuario de alto riesgo, todos los de sistemas lo usan, tiene la misma clave, tiene 626
	ALTER		
	EXECUTE		
	DEBUG		
	DELETE		

	INDEX		asignaciones de derechos sobre los recursos de información de la base de datos
	INSERT		
	UPDATE		
	REFERENCES		
	ON COMMIT REFRESH		
	QUERY REWRITE		
	FLASHBACK		
	EXECUTE		
XDB	EXECUTE	note714_T	usuario con uso específico por una sola vez

b. Los usuarios SUI3 y SUI5 presentan concentración de acceso a todos los recursos de información, estos usuarios son utilizados indistintamente por la Oficina Asesora de Planeación y Sistemas incurriendo en los siguientes riesgos:

- Cuando borren un registro no se puede establecer quien lo hizo
- Cuando borran un archivo o tabla no se puede establecer quien lo hizo
- Cuando modifican un registro de un archivo o tabla no se puede identificar quien lo hizo
- Cuando adicionan registros no se sabe quién lo hizo
- Un usuario puede estar logeado simultáneamente en varias estaciones.
- Estos usuarios tienen claves y password que varias personas conocen.
- En general si sucede un evento de cambio, borrado o adición de información no se puede establecer quien lo hizo.

3. OBSERVACIONES Y RECOMENDACIONES

3.1 Se recomienda actualizar el Plan de continuidad del negocio, tomando como referencia la Guía de MinTIC, actualizando a la fecha con los cambios y/o modificaciones de los sistemas de infraestructura y software que la Superintendencia de Economía Solidaria haya realizado y restablecer o redefinir los siguientes elementos del Plan de continuidad:

- Análisis del impacto al negocio (BIA por sus siglas en ingles),
- Sitio alterno del centro de datos,
- Plan de recuperación de desastres
- Punto objetivo de recuperación (RPO)
- Punto Tiempo objetivo de tiempo de recuperación (RTO)
- Objetivo mínimo de continuidad de negocio
- Recuperación de desastres de tecnología y telecomunicaciones

3.2 Rediseñar el manual de rendición de cuentas de SICSES para que sea una herramienta de apropiación del manejo del sistema y disminuya el soporte solicitado, aplicar los conceptos de usabilidad.

3.3 Ajustar el procedimiento de control de cambios a los sistemas de información que se desarrollan al interior de la Superintendencia de Economía Solidaria para que incluya en su flujo las buenas prácticas vigentes.

3.4 Actualizar y construir una política de copias de seguridad teniendo en cuenta los riesgos que maneja la información de cada sistema y como se mitigan realizando y probando cotidianamente las copias de seguridad.

3.5 Normalizar la asignación de usuarios a la base de datos con criterios funcionales de acuerdo con las atribuciones y responsabilidades de cada usuario y la asignación debe ser con el nombre del dominio de la Superintendencia, de tal suerte que los logs o bitácoras identifiquen a simple vista el usuario responsable.

3.6 Por último, se recomienda hacer una revisión general de las observaciones que se indicaron en cada uno de los puntos desarrollados en el presente informe, con el fin de que se implementen las acciones que sean requeridas para el mejoramiento del proceso.

Finalmente, se solicita dar respuesta por este mismo medio y en este mismo expediente, sobre las observaciones incluidas en el presente informe de auditoría, realizando la suscripción del Plan de Mejoramiento correspondiente por parte del líder del proceso dentro de los siete (7) días hábiles siguientes a partir de la fecha de remisión de conformidad con lo establecido en el parágrafo primero del artículo 2.2.21.4. del Decreto 1083 de 2015. Se adjunta el formato “F-COIN-016 Plan de Mejoramiento.

Cordialmente,

(Original Firmado)
MABEL ASTRID NEIRA YEPES
Jefe Oficina de Control Interno.

Elaboró: Rafael Luis Gabriel Vergara