SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

AUDITORIA BÁSICA CENTRO DE DATOS

OFICINA DE CONTROL INTERNO

Septiembre de 2019

Tabla de contenido

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. 20 – Auditoria Básica Centro de Computo, Data Center, Backups, la Oficina de Control Interno presenta el informe de auditoria básica de Auditoria Centro de Computo, Data Center, Backups.

1.2 OBJETIVO GENERAL

Verificar las buenas prácticas de infraestructura tecnológica se aplican.

1.3 OBJETIVOS ESPECIFICOS

- Confirmar la arquitectura tecnológica de servidores, comunicaciones, almacenamiento y continuidad del servicio de energía que se dispone.
- Revisa la rutina de copias de seguridad, disposición, riesgo y rotación de las mismas.
- Plan de continuidad
- Procesamiento alterno
- Acceso al centro de cómputo.
- Normas de seguridad

- Trazabilidad de eventos
- Control de aires, control de temperatura
- Revisar el control de cambios de la infraestructura a la luz de buenas prácticas como ITIL
- Confirmar estrategia de usuarios para el datacenter

1.4 ALCANCE

Se evaluó la gestión y el **estado** al día junio 13 del 2019 y la información entregada por la OAPS

1.5. METODOLOGIA

- Se seleccionaron 7 áreas relacionadas con el centro de datos así:

    - Seguridad Física
    - Seguridad de redes
    - Protocolos y servicios
    - Seguridad de usuario
    - Seguridad de datos
    - Contraseñas
    - Administración del sistema

- Se desarrolló por cada área a evaluar cuestionarios, los cuales en total se seleccionaron 77 preguntas, para establecer el estado de cada una de ellas.

- Se realizaron entrevistas con el los funcionarios relacionados como son: el jefe de sistemas, el oficial de seguridad, el asistente del centro de datos y el encargado de las herramientas de seguridad.

- Se realizó visita al centro de datos en compañía de un funcionario del área de OAPS.

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

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 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. Para instalar software en algún servidor, se deja registro y evidencia de su instalación por correo, pero no se diligencia una bitácora física o virtual que a simple vista se vea la cronología de las instalaciones realizadas, quien las realizó, cuál fue el motivo, a que versión pertenece, toda esta trazabilidad es necesaria al momento de evaluar un evento de mal funcionamiento o de seguridad.

2.2. No se revisa periódicamente la actividad inusual de usuarios, se efectúa por evento o solicitud presentada por un Directivo a la OAPS, las herramientas PCSecure, Dominio y Fortinet generan los informes a solicitud para analizar, sin embargo no se aprovecha rutinariamente estas facilidades para identificar posibles intentos de acceso no autorizado o uso indebido de recursos por un usuario.

2.3 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. 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.

c. 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.

2.4. 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. Las copias de seguridad realizadas en cinta no se guardan en sitios alternos fuera de las instalaciones de la Superintendencia.

e. No se realizan pruebas de aseguramiento de las copias de seguridad, esto significa que se realizan las copias de seguridad en forma rutinaria, pero no se comprueba que la restauración de la cinta se pueda realizar por completo.

2.5. No existe un procedimiento escrito y oficializado del manejo de las claves de los servidores, swiches y demás recursos asociados al centro de datos que requieran clave para su acceso, ejecutando cada vez que se requieren diferentes actividades que pueden incurrir en perdida de una clave de un servidor.

2.6. En mesa de servicio no se recopilan las fallas detectadas por los usuarios para realizar análisis e implementar planes de mejora, para que se disminuyan las solicitudes de los usuarios por las que más frecuencia reclaman servicio.

2.7. Para cambios de las máquinas del centro de datos, se deja registro y evidencia de su instalación por correo, pero no se diligencia una bitácora física o virtual que a simple vista se vea la cronología de los cambios realizados, quien las realizó, cuál fue el motivo, toda esta trazabilidad es necesaria al momento de evaluar un evento de mal funcionamiento o de seguridad.

2.8. No Existen reglas y normas del centro de computo definidas mediante un manual o instructivo que esté disponible en Isolucion.

2.8. La OAPS no tiene acuerdos de niveles de servicio SLA con la Superintendencia, de tal suerte que se pueda medir y se castigue de alguna manera los incumplimientos, los SLA deben ser planteados por cada servicio (eSigna, fábrica de reportes, BI, internet, correo electrónico, isolucion, intranet, pagina WEB, etc), e indicar en tiempos de atención de 7x24 durante un mes, un semestre y el año el nivel de servicio que mínimo debe estar por el 99,5% y que este informe sea presentado a la alta dirección.

3. OBSERVACIONES Y RECOMENDACIONES

3.1 Implementar el registro en bitácora del centro de datos para eventos de instalación de software y hardware.

3.2 Desarrollar por escrito los manuales e instructivos necesarios alrededor del centro de datos.

3.3 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

3.4 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 Acordar con la administración los niveles de acuerdo de servicios SLA.

3.6 Realizar pruebas de restauración a las cintas de las copias de seguridad como procedimiento rutinario.

3.7 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.

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