ICA 27/09/2023 12:08
Al Contestar cite este No.: **20233120208**
Origen: Oficina de Control Interno
Destino: Gerencia General
Anexos: Fol:4

MEMORANDO

11.100.4
Bogotá,

PARA: **JUAN FERNANDO ROA ORTIZ**
Gerencia General

DE: OFICINA DE CONTROL INTERNO

ASUNTO: FUNCIÓN PREVENTIVA - PLAN DE CONTINUIDAD DEL NEGOCIO

Doctor Roa, reciba un cordial saludo.

En atención al cumplimiento de las funciones de la Oficina de Control Interno, establecidas por el ordenamiento jurídico a través de la ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones" y en especial los literales:

d) Verificar que los controles asociados con todas y cada una de las actividades de la organización, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad;

f) Servir de apoyo a los directivos en el proceso de toma de decisiones, a fin de que se obtengan los resultados esperados.

Y en concordancia con la normatividad establecida para planes de continuidad, como lo son:

- ISO 27001:2022, Norma Técnica de Seguridad de la Información. Capítulo 5.3 Preparación de las TIC para la continuidad de la actividad.
- NTC/ISO 22301:2019 Norma internacional para sistemas de gestión para la continuidad de negocio.
- Decreto 1078 de 2015 Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea. Art.2.2.9.1.1.3, literal 10. "10. Proactividad: Los sujetos obligados a la Política de Gobierno Digital desarrollarán capacidades que les permitan anticiparse a las necesidades de los ciudadanos y, en general, los habitantes del territorio nacional, en la prestación de servicios de calidad y mitigar riesgos asociados a la continuidad y disponibilidad de estos, así como la identificación de riesgos asociados a la regulación del sector."
- Decreto 1072 de 2015; Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) en su artículo 2.2.4.6.4 que indica "…anticipar, reconocer, evaluar y controlar los riesgos que

puedan afectar la seguridad y la salud en el trabajo."

- Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres.
- Con el Modelo Integrado de Planeación y Gestión – MIPG, a través de la 3ª. Dimensión: Gestión con valores para resultados, en la que la estrategia de continuidad del negocio institucional deberá facilitar la integración de las estrategias preservación de la seguridad y la vida de los grupos de valor de la Entidad.

Es así que, el Instituto al no tener estructurado un Plan de Continuidad o un Plan de Recuperación de Desastres de la Información, no está garantizando mantener las operaciones y aplicativos que salvaguardan integralmente la información de la entidad, con las siguientes consecuencias posibles:

- No contar con una rápida recuperación de las aplicaciones y servicios en caso de un evento o desastre.
- No asegurar que el impacto del evento, permita continuar con la operación del Instituto.
- No contar con la asignación de recursos de personal, equipos tecnológicos y/o lugar de respaldo para continuar operando con el mínimo impacto.
- No prestar en un tiempo mínimo las operaciones principales del Instituto, al presentarse una emergencia.
- Presentar falla en la gestión de la seguridad y privacidad de la información, en caso de: ataques cibernéticos, incendios, inundaciones, pandemias, accidentes o errores humanos.

Por lo anteriormente expuesto, la Oficina de Control Interno, ha adelantado las siguientes gestiones sobre este tema:

Vigencia 2020:

Mediante memorando sisad No. 20203115251 de fecha 12/06/2020 la Oficina de Control Interno elevó ante la Gerencia General función preventiva a la falta del Plan de Continuidad del Negocio del Instituto.

Vigencia 2021:

Se realizó consulta a la Oficina Asesora de Planeación y a la Oficina de Tecnologías de la Información, mediante memorando N°20213113698el día 03/06/2021y reiterado por sisad 202013114460 el día 11/06/2021, sin embargo, a esa fecha, dichas Oficinas no dieron respuesta de avance a la solicitud.

Posteriormente, mediante memorando sisad No. 20213116259 de fecha 29/06/2021, la Oficina de Control Interno elevó ante la Gerencia General, la segunda función preventiva a la falta de un Plan de Continuidad del Negocio del Instituto.

Vigencia 2023:

Fue solicitado avance sobre el diseño e implementación del Plan de Continuidad del Negocio del Instituto o Plan de Recuperación de Desastres de la Información, a la Oficina Asesora de Planeación, mediante sisad 20233116922 del 28/08/2023 y a la Oficina de Tecnologías de la Información mediante sisad 20233116921 del 28/08/2023.

Por parte de la Oficina de Tecnologías de Información, la respuesta se recibió por sisad 20233117399 del 31/08/2023, quienes indicaron que dentro del Plan Anual de Adquisiciones 2023, se contratará una firma externa, con presupuesto de $500 millones para preparar un Plan de Continuidad para el Instituto.

Por parte de la Oficina Asesora de Planeación, se recibió respuesta sisad 20233120133 del 26/09/2023, en el cual remitieron las preguntas y respuestas No. 175 y 176 del formulario FURAG vigencia 2022, y fue diligenciado en junio 2023, que a continuación se detallan:

·**Pregunta FURAG 175**. Para asegurar la continuidad de la seguridad de la información la entidad:

"Contó con un plan de continuidad del negocio o plan de recuperación de desastres definido, documentado y aprobado por la Alta Dirección y han realizado pruebas de continuidad…"

Respuesta ICA: No tiene un plan de continuidad de negocio o un plan de recuperación de desastres.

·**Pregunta FURAG 176**. *¿La entidad realizó pruebas de recuperación de información y continuidad de los sistemas de información críticos en la vigencia 2022?"*

Respuesta ICA: El sistema inhabilitó la pregunta 176, por la respuesta de la pregunta 175.

Por lo anterior, la Oficina de Control Interno eleva ante la Gerencia General función preventiva asociada al Plan de Continuidad para el Instituto y plantea las siguientes recomendaciones:

- Propender porque el proyecto de seleccionar una firma externa para iniciar el diseño e implementación de un Plan de Continuidad se inicie dentro del segundo semestre 2023, como

se indica en el Plan Anual de Adquisiciones.

- Desarrollar el Plan de Continuidad o Plan de Recuperación de Desastres de Información, conforme al marco normativo vigente para este tipo de planes.
- Como anexo del Plan, incluir un cronograma de pruebas o simulacro, las cuales deben realizarse periódicamente. Este cronograma debe mantenerse actualizado con los recursos de personal y tecnológicos.
- Publicar y socializar el Plan de Continuidad que se aprueba para el Instituto, para conocimiento del personal del ICA.
- Es importante evaluar los riesgos e impactos por la pérdida de continuidad de la operación de la entidad y actualizar el mapa de Riesgos Institucional conforme a los riesgos identificados a un Plan de Continuidad, como lo plantea la ISO 27001:2022 en su capítulo 6.
- Dada la importancia de este tema, se requiere una articulación interinstitucional de la entidad, donde no sea la Oficina de Tecnologías de la Información, la única responsable.

Por parte de la Oficina de Control Interno, estaremos atentos para cualquier colaboración que sea pertinente,

Atentamente,

JUAN FERNANDO PALACIO ORTIZ
Jefe Oficina Control Interno

Respuesta a: Radicación No. 20233116921 del: 28/08/2023
C.C.: Oficina Asesora de Planeación
Oficina de Tecnologias de Información
Elaboró: Daniel Toro Castañeda