Función Pública

Seguimiento Plan Estratégico de Continuidad del Negocio

Evaluación Independiente

OFICINA CONTROL INTERNO

Versión 1

Diciembre 2024

Objetivo

Evaluar por parte de la Oficina de Control Interno, el estado de cumplimiento del Plan Estratégico de Continuidad de Negocio – PECN en Función Pública, acorde con las mejores prácticas establecidas en la norma ISO 22301 – 2019 para sistemas de gestión de continuidad de negocio.

Alcance

Se evaluará el grado de cumplimiento a las actividades inmersas en el plan estratégico de continuidad del Departamento Administrativo de la Función pública, versión 1 de enero 2024, cuyo objetivo está en “implementar los lineamientos establecidos en la norma ISO/IEC 22301 dentro del Departamento Administrativo de la Función Pública, con el fin de brindar disponibilidad a los servicios misionales de la Entidad”. Las actividades determinadas en el plan son:

- Establecer las bases de datos y aplicaciones misionales de la organización
- Establecer los requerimientos legales, normativos y de cumplimiento
- Documentar el sistema de gestión de continuidad del negocio
- Documentar los ejercicios de recuperación ante el desastre
- Documentar los planes y las acciones requeridas para restablecer las operaciones misionales de la Función Publica
- Planificar y llevar a cabo auditorías internas del SGSI
- Emprender revisiones por la dirección del SGSI regularmente
- Aplicar la Mejora Continua al Sistema de Gestión de Seguridad de la Información

1. Resultados del seguimiento

No.	Actividades	Meta/hito	Observaciones OCI
1	Establecer las bases de datos y aplicaciones misionales de la organización	1. Matriz de riesgos que afecten la disponibilidad de los servicios misionales actualizada 2. Listado de bases de datos y aplicaciones misionales documentada 3. Matriz de infraestructura de soporte a bases de datos y/o aplicaciones misionales documentada	1. Se evidenciaron los siguientes riesgos orientados a la disponibilidad de la información o de los sistemas de información en la sábana de riesgos registrada en el SGI: -057 Aprobado, 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, proceso TI. -099 aprobado, Posibilidad de pérdida reputacional por quejas de los grupos de valor debido a la no disponibilidad de la información gestionada por el proceso, en el archivo en físico o digital administrado y almacenado por el grupo de apoyo a la gestión meritocrática. Proceso Acción Integral en la Administración Pública Nacional y Territorial De otro lado, hay un plan de Tratamiento de Riesgos de Seguridad 2024 Versión 1 - enero 31 2024, en el cual se estableció la actividad de analizar y actualizar los riesgos y controles de seguridad digital, dejando como meta la Actualización de mapa de riesgo de seguridad digital. 2. En el documento denominado “2024-05-15_Anexo_analisis_impacto_negocio”, se evidencia el listado de aplicaciones, sitios web o bases de datos que permiten prestar los servicios ante la ciudadanía o atención a solicitudes de entes de control, entre las que se encuentran a nivel misional externo: - FURAG - SIGEP II - SUIT

No.	Actividades	Meta/hito	Observaciones OCI
			- MIPG - SIE A nivel misional interno: - ORFEO - VPN - PDF - FIRMA ELECTRONICA - OFFICE - CORREO ELECTRONICO - YAKSA - ASSURANC - KACTUS - PROACTIVANET - PORTAL WEB - CRM - NEON - EVA 3. Trabajo realizado mancomunadamente entre la OTIC y la OAP , donde se evidencia un formato de inventario de activos actualizado a junio de 2024, en el cual está registrada toda la infraestructura de soporte a las Bases de datos y aplicaciones de FP.
2	Establecer los requerimientos legales, normativos y de cumplimiento	1.Documento anexo con niveles de prestación de los servicios misionales documentados 2.Anexo normativo asociado a la disponibilidad de los servicios de función pública documentado.	1. En el documento de análisis de impacto del negocio no se evidencian dichos niveles o ANS , no obstante, se tienen por separado para cada sistema misional los acuerdos de nivel de servicios establecidos acorde con los contratos base que los soportan. 2.*No se evidencia el anexo normativo planeado en el PECN*. En el gestor normativo no aparece ningún elemento relacionado con el tema de disponibilidad de los servicios de FP y en los Requisitos Legales de Direccionamiento Estratégico registrados en el SIPG, tampoco.

No.	Actividades	Meta/hito	Observaciones OCI
3	Documentar el sistema de gestión de continuidad del negocio	1.Documento técnico del sistema de continuidad actualizado. 2. Matriz de escalamiento de funcionarios que deben intervenir en el caso de interrupción documentada e integrada al plan de continuidad 3. Matriz de responsabilidades ante la disrupción identificada y socializada 4.Matriz de asignación de recursos	1. El Documento técnico del Sistema de continuidad se encuentra en proceso de revisión, no ha sido actualizado aún. Se evidencia el Documento Técnico del Plan de continuidad del Negocio, versión 5 de enero 2023, con algunos comentarios y ajustes por parte del CISO. 2. Se despliega en el documento técnico mencionado, las estrategias para cada escenario (Emergencia social, Desastre natural y colapso de infraestructuras, Tecnológico, Financiero y Sanitario, donde se puede evidenciar el líder de respuesta y las acciones a desarrollar por parte del equipo de respuesta asociado. 3. En el documento denominado “2024-05-15_Anexo_analisis_impacto_negocio”, se evidencia la respectiva matriz de escalamiento en el siguiente orden: ✓ Comité de crisis ✓ Subdirección ✓ Dirección de la Oficina Asesora de Planeación ✓ Dirección de la Oficina de Tecnología y Comunicaciones ✓ Oficial de seguridad de la Información ✓ Direcciones de los procesos afectados 4. Se despliega en el documento técnico mencionado, las estrategias para cada escenario (Emergencia social, Desastre natural y colapso de infraestructuras, Tecnológico, Financiero y Sanitario, donde se establece dentro de las actividades el manejo de los recursos humanos y financieros disponibles
4	Documentar los ejercicios de recuperación ante el desastre	1. Ficha de escenarios de disrupción actualizados 2. Documento de respaldo base de datos documentado y revisado 3. Plan de gestión del cambio documentado e implementado	Para esta vigencia, se efectuó ejercicio de recuperación para la herramienta de manejo de nómina Kactus, y se están empezando a organizar las pruebas de ORFEO. Para sistemas misionales no se programaron pruebas esta vigencia.

No.	Actividades	Meta/hito	Observaciones OCI
			1. Se evidencian las fichas respectivas por cada escenario de disrupción (Emergencia social, desastre natural, desastre tecnológico, Financiero y Pandemia), en las cuales se especifican por cada fase de detección, activación, plan de operación alterno y resolución del incidente, la gestión respectiva por responsable. 4. Documento específico de respaldo de BD documentado y revisado no se evidencia. En el documento del plan de recuperación del servicio se describe en el numeral 4 como reanudar el trabajo rápidamente después de un incidente no planificado, especificando el proceso de restauración del servidor de aplicaciones, donde se detalla la instalación de las bases de datos de Oracle. 5. No se pudo evidenciar un Plan de gestión del cambio documentado e implementado. Nota: Si bien está documentada toda la prueba de recorrido efectuada al ejercicio de recuperación de la herramienta KACTUS, esta se incluyó directamente sobre el DRP del mismo sistema, debería mantenerse un documento independiente y con las fechas de ejecución, programación, gestión y resultados (Lecciones aprendidas)
5	Documentar los planes y las acciones requeridas para restablecer las operaciones misionales de la Función Publica	1.Ficha técnica de ejercicios de Continuidad adelantados 2. Cronograma para el ejercicio de restablecimiento operativo 3. Resultados de las pruebas	Por parte de la OTIC se realizó el DRP de las bases de datos que están en producción. En este documento versión 1 generado el pasado mes de agosto, se describe la implementación técnica del DRP para las bases de datos, desde el datacenter de nube privada y datacenter del DAFP. De otro lado, se encontraron los DRP actualizados de los sistemas misionales SIGEP, SUIT, FURAG y Aplicativo por la Integridad, los cuales tienen por objetivo

No.	Actividades	Meta/hito	Observaciones OCI
			general establecer el plan de recuperación para cada Sistema en caso de una falla que genere una indisponibilidad del sistema ante la eventualidad de incidentes, accidentes y/o estados de emergencia. En cada DRP se establece la gestión por cada una de las etapas estipuladas por la norma ISO 22301:2019 (Planear, Hacer, Verificar y Mejora continua) Los DRP evidenciados fueron: - SIGEP II, versión 2 de mayo 2024 - SUIT III, versión 2 de mayo 2024 - FURAG, versión 4 de mayo 2024 - Aplicativo por la Integridad, versión 2 de mayo 2024 *No obstante, y de acuerdo con las metas/hitos propuestos no se evidencia gestión de pruebas para estos sistemas durante esta vigencia.* *Tampoco estos DRPs actualizados han sido publicados en el SIPG. En Proativanet solo está actualizado el del Sistema SUIT.*
6	Planificar y llevar a cabo auditorías internas del SGSI	Auditorías internas del SGSI realizadas y documentadas	A pesar que no se han efectuado auditorias o seguimientos al SGSI por parte de la OCI, si se efectúan evaluaciones a la seguridad de acceso y algunos temas de asegurabilidad de las plataformas sobre las que se operan los sistemas misionales y demás herramientas, así como a la gestión de continuidad de negocio en cada una de las auditorias o seguimientos técnicos a los sistemas de la entidad que estén programados en el plan anual de la vigencia respectiva.
7	Emprender revisiones por la dirección del SGSI regularmente	Informe del seguimiento realizado por la dirección al SGSI	No se ha efectuado

No.	Actividades	Meta/hito	Observaciones OCI
8	Aplicar la Mejora Continua al Sistema de Gestión de Seguridad de la Información	Planes de acción frente a los hallazgos o levantamientos como resultado de las auditorías internas o de entes de control documentados y realizados	Los planes de mejora se encuentran en tratamiento acorde con el procedimiento interno vigente.

Conclusiones y recomendaciones

1. Acorde con lo establecido en el plan de Tratamiento de Riesgos de Seguridad, y previo análisis de los procesos intervinientes, se considera importante incluir en la matriz de riesgos de la entidad, aquellos que afecten la disponibilidad de los servicios misionales, teniendo en cuenta a todas las Direcciones Técnicas, no solo la OTIC; esto con el fin que se implementen planes de recuperación de desastres robustos y articulados que contemplen toda la gestión operativa y técnica ante una indisponibilidad del servicio y fortalezca además el uso y apropiación de la tecnología de información. (Actividad 1, Hito 1 PECN).

2. Respecto a la actividad 2 “Establecer los requerimientos legales, normativos y de cumplimiento”, hito 2 del PECN, relacionado con la generación de un anexo normativo asociado a la disponibilidad de los servicios del Departamento, sobre el cual no pudo ser evidenciado su cumplimiento, es importante analizar su inclusión en la generación del PECN 2025.

3. Se debe actualizar, publicar y socializar la última versión del Documento Técnico del Plan de Continuidad del Negocio en la página web del DAFP. (Actividad 3 Hito 1 del PECN).

4. Con relación a la actividad 4 “Documentar los ejercicios de recuperación ante el desastre“, hito 3 relacionado con la implementación de un Plan de gestión del cambio

documentado e implementado, el cual no pudo ser evidenciado, se recomienda analizar su inclusión en la generación del PECN 2025.

5. Respecto a los ejercicios de recuperación ante desastre que se han venido efectuando, y en específico con la herramienta KACTUS, es importante que los resultados queden registrados en un documento independiente donde se especifiquen las fechas de ejecución, programación, gestión, resultados obtenidos y lecciones aprendidas.

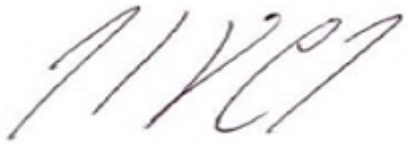
6. Para la actividad 5 del PECN, es importante que para la vigencia 2025, se desarrollen los hitos que se habían establecido para las operaciones y sistemas misionales relacionados con los ejercicios de continuidad y sus resultados. Se recalca de nuevo esta gestión que aún no ha podido ser ejecutada por la Entidad, y que como se ha expresado, permite medir la efectividad de los planes establecidos para mitigar el riesgo de perdidas en la continuidad de la operación.

   De otra parte, publicar y socializar en el SIPG y en la mesa de servicio Proactivanet los DRPs de los cuatro sistemas misionales (SIGEP, SUIT, FURAG y Aplicativo por la Integridad) actualizados en el mes de mayo de la presente vigencia.

7. Como parte de la mejora continua del SGSI recomendada por la norma ISO 27001, se debe adelantar en la próxima vigencia el procedimiento de revisión por la Dirección, la cual permite garantizar que el SGSI y sus objetivos continúen siendo adecuados y efectivos y así mismo, evaluar la validez de los problemas identificados y los riesgos de la Entidad. (Actividad 7 del PECN)

8. Mantener la continuidad en la gestión a los planes de mejoramiento derivados del SGSI, tal y como se ha venido efectuando a través de la vigencia.

9. Finalmente, a raíz de la pérdida del recurso humano asignado a la labor de Oficial de Seguridad de la Oficina Asesora de Planeación, sucedida hacia el tercer trimestre de la vigencia actual, se vio afectado en parte el cumplimiento del PECN para la vigencia 2024, pese al esfuerzo aportado desde la OTIC a través del profesional de seguridad de la información de dicha dependencia; por ende, se recomienda a la Alta Dirección del Departamento, considerar la asignación y permanencia en lo posible del recurso humano mencionado para futuras vigencias, esto con el fin de mantener la gestión sobre el diseño de estrategias y políticas de seguridad, así como al cumplimiento de la normativa asociada, entre otras.



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

SEGUIMIENTO PLAN ESTRATÉGICO DE CONTINUIDAD DEL NEGOCIO

Versión 01
Proceso de Evaluación Independiente
Diciembre 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 5 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)