Función Pública

INFORME DE SEGUIMIENTO AL PLAN ESTRATÉGICO DE CONTINUIDAD DEL NEGOCIO

Evaluación Independiente

OFICINA CONTROL INTERNO

Versión 01

Agosto de 2026

Objetivo

Verificar y evaluar por parte de la Oficina de Control Interno el estado actual de cumplimiento del Plan Estratégico de Continuidad de Negocio – PECN vigencia 2026 en Función Pública, acorde con las mejores prácticas establecidas en la norma ISO 22301 – 2019 para sistemas de gestión de continuidad de negocio.

Es importante mencionar que las observaciones registradas en el presente informe de seguimiento coadyuvan a fortalecer el ambiente de control de la seguridad de la información al interior de la entidad.

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 2026, el cual busca "*Garantizar la continuidad operativa de las funciones y procesos críticos de la entidad ante la ocurrencia de incidentes, crisis o eventos disruptivos, mediante la implementación de estrategias y capacidades de respuesta, recuperación y resiliencia, minimizando el impacto sobre la entidad, sus funcionarios, usuarios y demás partes interesadas, en conformidad con las normas ISO 22301 e ISO 27031.*". Las actividades registradas en el plan publicado en la sección de transparencia de la página WEB de Función Pública son:

- Identificar, clasificar y documentar las bases de datos y aplicaciones misionales de la entidad.
- Establecer analizar y documentar los requerimientos legales, normativos y de cumplimiento aplicables a la continuidad del negocio.
- Documentar el sistema de gestión de continuidad del negocio.
- Diseñar y documentar el Plan de gestión del cambio documentado
- Actualizar los Planes de recuperación de los Sistemas de Información y Aplicativos Críticos.

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)

1. Resultados del seguimiento

A continuación, se presenta el detalle del resultado de la verificación al estado actual de cada una de las actividades consignadas en el Plan Estratégico de Continuidad del Negocio - PECN del Departamento Administrativo de Función Pública – DAFP vigencia 2026.

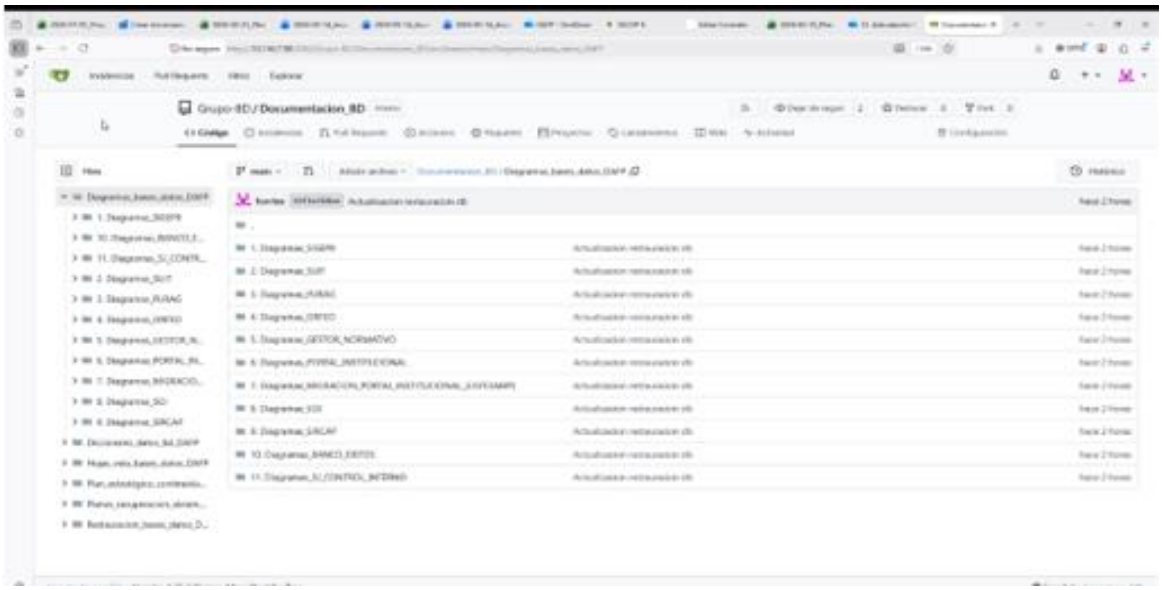
1.1. Actividad 1: Identificar, clasificar y documentar las bases de datos y aplicaciones misionales de la entidad

Responsable(s): Responsable BD OTIC

1.1.1. Hito1: Elaborar un inventario de las bases de datos misionales

Estado Actual

Se tiene un servidor interno a través del software de código abierto GITEA, para alojar el control y trazabilidad de versiones de desarrollo de software, con el objeto de centralizar el código y desarrollo que se efectúan en los diferentes aplicativos de la Entidad, en él se pudo evidenciar toda la información (Diagramas y Hojas de vida de las Bases de Datos – BD) correspondiente a las BD de la entidad de los sistemas misionales (SIGEP, SUIT y FURAG) y de apoyo.



Fuente: software GITEA bases de datos

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

Página web:
www.funcionpublica.gov.co

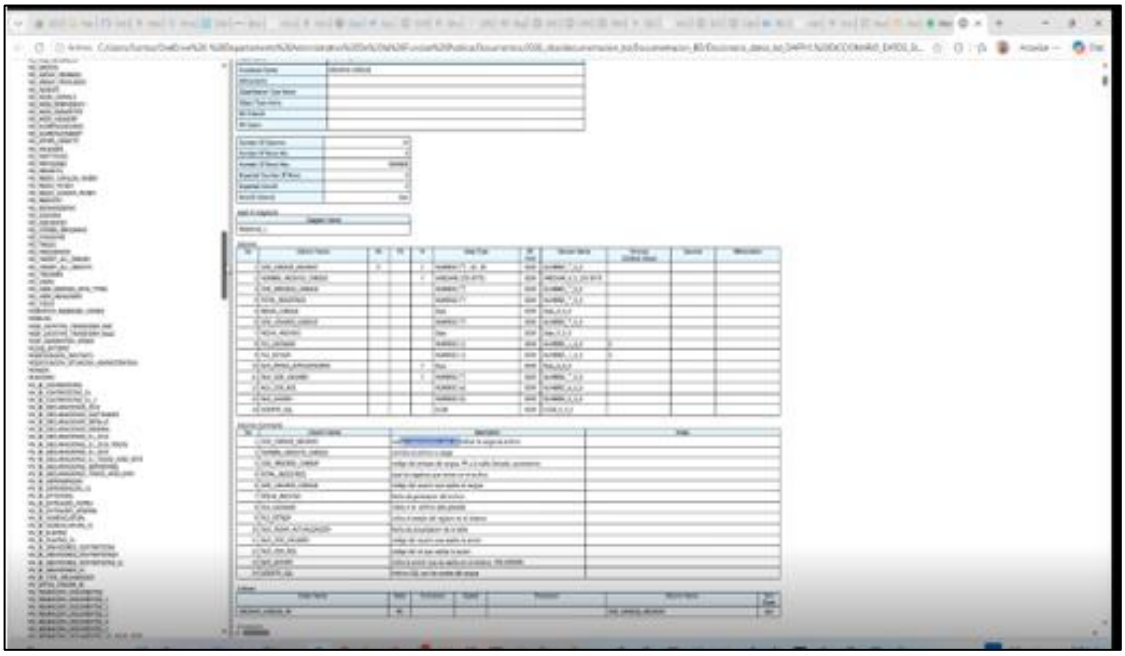
Email:
eva@funcionpublica.gov.co

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)

Esta herramienta maneja roles de consulta a las bases de datos (Productivas, QA y desarrollo) sobre los cuales se brinda la información a los diferentes ingenieros que gestionan desarrollos de software sobre los sistemas de información existentes.

Por ejemplo, a nivel de BD, en la herramienta estan registrados:

- ✓ Los Diagramas de cada BD, dónde se pueden observar los modelos conceptuales, relacionales y lógicos por cada BD
- ✓ Los Diccionarios de datos con sus objetos y descripciones específicas.(Ejemplo siguiente imagen)



Fuente: Diccionario de datos SIGEP, extraído de GTEA (30 de julio 2026)

- ✓ Hojas de vida de cada BD (Características técnicas de cada BD), con el fin de que en los procesos de recuperación se tenga el historial de la BD, S.O, versionamiento, datafiles , vistas, entre muchos más atributos técnicos.

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)

1.1.2. Hito 2: Definir los RTO (tiempo máximo de recuperación) y RPO (pérdida máxima de datos aceptable) para cada base de datos y aplicación crítica.

Estado actual:

Verificando la definición de los RTO y RPO al interior de los planes de recuperación de desastres para los sistemas misionales y de apoyo existentes, se encontró lo siguiente:

SISTEMA	RPO	RTO
SIGEP	No está claramente definido	No está claramente definido
SUIT	Máquinas virtuales 15 días Bases de datos 2 días	3 días
FURAG	No está claramente definido	No está claramente definido
KACTUS	No está claramente definido	No está claramente definido
APLICATIVO POR LA INTEGRIDAD	No está claramente definido	No está claramente definido
ORFEO	No está claramente definido	No está claramente definido
DRP BASES DE DATOS	4 Horas	15 minutos cada db
BASES DE DATOS ORACLE	4 horas	1 hora

Como se puede observar, todavía no han sido definidos los RTO y RPO para la mayoría de DRPs, actividad que encuentra en proceso por parte de la OTIC.

Control de gestión sobre la actividad/hitos:

Las actividades desempeñadas no estan concentradas en un entregable dentro de la planeación institucional en el SGI, lo cual no permite ver la trazabilidad y medición de la gestión del responsable en el sistema.

Recomendaciones

1. Mantener la continuidad en la definición de los RPO y RTO por sistema misional y de apoyo, acorde como lo define el Hito (base de datos y aplicación). Se recuerda

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)

que estos objetivos son métricas clave en la continuidad del negocio, las cuales permiten una planificación precisa de los respaldos, minimizar las pérdidas económicas y asegurar una rápida restauración operativa ante un fallo o desastre tecnológico.

2. Con el fin de conservar la trazabilidad y control de la gestión de las actividades e hitos del PECN, se deben incorporar las actividades determinadas para las bases de datos en el módulo de planeación institucional del SGI, manteniendo su respectivo registro.

1.2. Actividad 2: Establecer analizar y documentar los requerimientos legales, normativos y de cumplimiento aplicables a la continuidad del negocio

Responsables: OTIC

1.2.1. Hito 1: Documento anexo que contiene los niveles de prestación de los servicios misionales debidamente documentados.

Estado actual:

Actualmente, la OTIC maneja tres niveles de control sobre la disponibilidad de los sistemas misionales:

- Informe mensual de disponibilidad de la infraestructura (Interoperabilidad), el cual tiene por objetivo “Presentar las tareas del grupo enfocándose a la gestión de los servicios para mantener e implementar los procesos de interoperabilidad de los sistemas de información (SIGEP-SUIT-VEEDURÍAS) con las entidades con las cuales el DAFP tiene convenios de intercambio de información”, en este informe se mantiene información del indicador de disponibilidad de la infraestructura (ver ejemplo siguiente imagen), como lo había esta Oficina recomendado en el seguimiento a la estrategia de Gobierno Digital en la presente vigencia.

1.5.6. Indicador de disponibilidad de Interoperabilidad

En este periodo se logra una disponibilidad de 100.00%.

#	Indicador Disponibilidad
Julio	100,00%

Ilustración 2 Indicador de disponibilidad

Fuente: Informe trabajo grupo interoperabilidad, julio 2026

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)

Los informes mencionados se evidencian en la ruta: \\yaksa\10031GSI\2026\DOCUMENTOS_APOYO\INTEROPERABILIDAD\DOCUMENTOS\INFORMES.

- Bitácora de interrupciones de servicio no programadas de los sistemas misionales, a manera de indicador sobre la calidad del servicio. Esta bitácora se maneja para los sistemas misionales SUIT y SIGEP, tratando de tener un soporte de trazabilidad e histórico de los niveles de disponibilidad del servicio.

  Para SUIT se evidencia la bitácora respectiva, donde se registra por día y hora la disponibilidad en el servicio de los ambientes de producción, pruebas y capacitación, cuando se reporta una falla, como se puede observar en la siguiente imagen:

FECHA	HORA	PRODUCCION	PRUEBAS	CAPACITACION	OBSERVACIONES
MIÉRCOLES 1/7/2026	8:00	OK	OK	OK	SIN NOVEDAD
	8:30	OK	OK	OK	SIN NOVEDAD
	9:00	OK	OK	OK	SIN NOVEDAD
	9:30	OK	OK	OK	SIN NOVEDAD
	10:00	OK	OK	OK	SIN NOVEDAD
	10:30	OK	OK	OK	SIN NOVEDAD
	11:00	OK	OK	OK	SIN NOVEDAD
	11:30	OK	OK	OK	SIN NOVEDAD
	12:00	OK	OK	OK	SIN NOVEDAD
	12:30	OK	OK	OK	SIN NOVEDAD
	13:00	OK	OK	OK	SIN NOVEDAD
	14:00	OK	OK	OK	SIN NOVEDAD
	14:30	OK	OK	OK	SIN NOVEDAD
	15:00	OK	OK	OK	SIN NOVEDAD
	15:30	OK	OK	OK	SIN NOVEDAD
	16:00	OK	OK	OK	SIN NOVEDAD
	16:30	OK	OK	OK	SIN NOVEDAD
	17:00	OK	OK	OK	SIN NOVEDAD
	17:30	OK	OK	OK	SIN NOVEDAD

Fuente: Bitácora de monitoreo diario de disponibilidad SUIT enero.- julio 2026

Esta bitácora se evidenció en la ruta: \\yaksa.dafp.local\10031GSI\2026\TRD\PROYECTOS\CONSTRUCCION_MANTENIMIENTO_SW\SUIT\INFORME_SEGUIMIENTO

Para SIGEP, se gestiona otro tipo de bitácora, un poco más detallada que contiene entre otra la siguiente información: Fecha del incidente, Hora inicio, Hora fin, Tipo de Incidente,

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)

Descripción del incidente, Solución, Usuarios atendieron caso. (Ver siguiente imagen de ejemplo).

9/01/2025	15:00	16:00	Inestibilidad	Se presento caida del sistema, afectando el ingreso a la plataforma por los usuarios, esto se desprende de consultas que se realizan a inicio del año por las entidades	Reinicio de servicios se devide el ajuste de las consultas junto al proveedor para optimizar los servicios	Mesa Tecnica;: Jefe OTIC: Jhon Ricardo Morales Franco Lider: Lucy Villaraga Equipo tecnico: Ingenieros Funcion Publica- Profesional Especializado: Lida Viviana Pineda Tecnico: Andres Soto- - Dario Rojas y AND y ADA
13/01/2025	9:00	12:00	Inestibilidad	Se presenta problemas con la realización de consultas de reportes, y se presenta problema de rendimiento enla base de datos	Reinicio de servicios Se debe validar el consumo por el sistema operativo	Mesa Tecnica;: Jefe OTIC: Jhon Ricardo Morales Franco Lider: Lucy Villaraga Equipo tecnico: Ingenieros Funcion Publica- Profesional Especializado: Lida Viviana Pineda Tecnico: Andres Soto- - Dario Rojas y AND y ADA
13/01/2025		16:00	Inestibilidad	Se presenta problemas con la realización de consultas de reportes, y se presenta problema de rendimiento enla base de datos	Se debe validar el consumo por el sistema operativo, como el manejo que esta teniendo el front con el back en relación a la comunicación con base de datos. y se empieza la activación de otro servidor para que soporte la	Mesa Tecnica;: Jefe OTIC: Jhon Ricardo Morales Franco Lider: Lucy Villaraga Equipo tecnico: Ingenieros Funcion Publica- Profesional Especializado: Lida Viviana Pineda Tecnico: Andres Soto- - Dario Rojas y AND y ADA

Fuente: Bitácora de monitoreo de disponibilidad SIGEPII enero.- mayo 2026

Para el sistema FURAG no se mantiene una bitácora, por cuanto solo está activo al usuario externo entre los meses de marzo y abril cuando se efectúa la medición. Además, es el único aplicativo que se tiene en nube publica, la cual maneja sus propios reportes y garantiza la total disponibilidad del servicio.

- Acuerdos de prestación de servicios – ANS de TI que están implementados actualmente, se encuentran registrados y controlados a través de la Mesa de Ayuda Proactivanet, como se pudo evidenciar en la herramienta. En ellos, se encuentra especificada entre otra la siguiente información:

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)

Código	Nombre	Descripción	Horas resolución
SLA-000055	SLA - SSP - 15 días	SLA - SSP - 15 días	127
SLA-000053	Cursos_Virtuales		127
SLA-000052	SLA_Furag_2días_Gestión de Incidencias	REQ 2024-040388	24
SLA-000051	SLA-SIGEPII-5-días	SLA-SIGEPII-5-días	40
SLA-000050	SLA-SIGEPII-2-días	SLA-SIGEPII-2-días	16
SLA-000049	SLA-SIGEPII-15-dias	SLA-SIGEPII-15-dias	120
SLA-000048	SLA-SIGEPII-6días		48
SLA-000047	SLA - ARCHIVO CENTRAL - 24 Horas		24
SLA-000046	SLA - ARCHIVO CENTRAL - 12 Horas		12
SLA-000045	SLA SUIT - 8 días	SLA, Según Matriz matriz entregadas el 7 de Octubre	72
SLA-000044	SLA - Nomina FP - GGA		24
SLA-000043	SLA - Nomina FP - OTIC		8
SLA-000042	SLA - Grupo de Mejoramiento Institucional-OAP - 3 días		28
SLA-000041	SLA-SIGEP-20-dias	SLA, para sigep para 20 días hábiles REQ 2020-048248	180
SLA-000040	SLA-Furag-8-días	Sla para furag de 8 días	68
SLA-000039	SLA-Furag-4-días	Sla para furag de 4 días	34
SLA-000038	SLA-Furag-5-días	Sla para furag de 5 días	42
SLA-000037	SLA-Furag-3-días	Sla de furag para 3 días	25
SLA-000035	SLA-Furag-10-días	Sla para furag de 10 días	85
SLA-000034	SLA - Gestor Normativo - 15 - días		127
SLA-000033	SLA - Banco de Gerentes - 15 días	SLA - Banco de Gerentes - 15 días	127
SLA-000032	SLA - SIGEPII- 20 días	Se amplia el tiempo a 20 día según REQ 2022-033153	160
SLA-000030	SLA SIE	niveles de servicio para SIE	90
SLA-000026	SLA 12 Horas - Gestión Administrativa	SLA 12 Horas - Gestión Administrativa	12
SLA-000025	SLA - Base de Datos		130
SLA-000024	SLA Intranet 8 horas hábiles		24
SLA-000023	SLA Intranet 5 Dias	Sla para el servicio de intranet de 5 días	45
SLA-000022	SLA Apoyo Administrativo 3 días	SLA Apoyo Administrativo 3 días	24
SLA-000021	Apoyo Administrativo 5 días	Apoyo Administrativo 5 días	40
SLA-000020	SLA Apoyo Administrativo 5 Horas	SLA, para la clasificación APOYO ADMINISTRATIVO que corresponde al Grupo de Apoyo Administrativo	5
SLA-000016	SLA - Conflicto de interés		127
SLA-000015	SLA-Soporte TI 3Horas	SLA para ser atendido en 3 horas de acuerdo a lo establecido por TI. Cambiado solo a Tecnicos de Soporte por instrucciones de la Coordinación de Infraestructura	3
SLA-000013	SLA EVA - 15 días	SLA solicitado a través del requerimiento REQ 2016-003276	360
SLA-000011	SLA - Sistema de reportes territoriales 15 días		2
SLA-000010	SLA SUIT - 15 días	SLA creado en REQ 2014-014687	135
SLA-000009	SLA SUIT - 10 días	SLA creado en REQ 2014-014687. Categoría Modelos incluida por REQ 2014-027287	90
SLA-000007	SLA SUIT - 4 días	SLA creado en REQ 2014-014687	36
SLA-000003	SLA T.I. - 24 horas	SLA para ser atendido en 24 horas de acuerdo al catalogo de servicios	24
SLA-000001	SLA T.I. - 12 horas	SLA para ser atendido en 12 horas de acuerdo a lo establecido por TI, por tratarse de los servicios críticos	12

Fuente: Reporte SLA´s Proactivanet julio 2026

Estos ANS actúan de manera automática controlados a través de la herramienta de Mesa de Ayuda Proactivanet para cada requerimiento que curse por la plataforma (Atención primer, segundo y tercer nivel).

Control de gestión sobre la actividad/hito:

Se mantiene un entregable en la planeación institucional denominado ”Sistemas de información misionales de Función Pública actualizados e interoperando”, en el cual se efectúa un registro de gestión bimensual. Para este primer semestre, los sistemas misionales SUIT, SIGEP y FURAG operaron de manera estable, con sus interoperabilidades funcionando en condiciones normales y eficientes. Las incidencias reportadas en cada una de las aplicaciones fueron gestionadas oportunamente, y las solicitudes de mejoras y controles de cambio requeridas por las áreas funcionales responsables fueron atendidas por la OTIC dentro de los tiempos establecidos.

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)

Recomendaciones

- Unificar la estructura de las bitácoras para SIGEP y SUIT, con el fin de gestionar y mantener el mismo tipo de información.

- Se debe generar un indicador de disponibilidad del servicio para los sistemas de información misionales, tal y como se está llevando actualmente el indicador de disponibilidad de la infraestructura, con la información registrada en las bitácoras mencionadas. Además, se debe registrar esta gestión en el entregable respectivo de la planeación institucional.

- Ajustar o redactar de mejor manera el entregable actual de la planeación institucional del SGI, orientándolo no solo a interoperabilidad sino a la disponibilidad de la infraestructura y del servicio (Sistemas Misionales).

- Unificar el informe de interoperabilidad actual, con la información del indicador de disponibilidad del servicio recomendado, con el fin de dar completez a la naturaleza del Hito.

1.3. Actividad 3: Documentar el sistema de gestión de continuidad del negocio

Responsables: CISO

1.3.1. Hito 1: Actualización de la Política de Continuidad del Negocio.

Estado actual

Actualmente está publicado en el SIPG en la sección de manuales y guías del proceso de Gestion de las tecnologías de la información, el “Manual de políticas de seguridad de la información”, versión 1 de noviembre de 2025, donde se detalla en el numeral 21, la Política en la Continuidad de Negocio, en el cual a nivel general se especifican las responsabilidades del Comité de Gestión y Desempeño Institucional CGDI, el Oficial de Seguridad de la Información Institucional y la OTIC, frente a:

i) Identificación de situaciones que sean consideradas como emergencia o desastre para Función Pública.
ii) Definición de las actuaciones ante la presencia de incidentes de seguridad y desastres.
iii) Coordinación de los temas relacionados con la continuidad del negocio y la recuperación ante cualquier tipo de desastre.

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)

iv) Gestión de los análisis de impacto a la entidad y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación.
v) Elaboración de un plan de recuperación ante desastres para el centro de datos de la entidad y un plan de contingencia para cada uno de los servicios, sistemas operativos y recurso informático existente.
vi) Coordinación de las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos al Comité Institucional de Gestión y Desempeño.

Por otro lado, se puede observar en el SIGP, la publicación de la Política General de Seguridad de la información versión 2 de marzo 2026. En esta política se pueden observar inmersos los siguientes elementos propios de la política de continuidad de negocio:

i) En los objetivos secundarios está el "Garantizar la continuidad del negocio, la gestión del cambio, gestión de accesos, gestión del riesgo y gestión de incidentes."
ii) En el alcance de la PGSI se incluyen los componentes de ciberseguridad, continuidad del negocio y protección de datos personales.
iii) Compromiso del DAFP en la inclusión de la aplicación de la protección de datos personales y garantiza así también la continuidad de los servicios misionales del Departamento.
iv) En la definición de roles y responsabilidades se especifican algunas actividades para la Alta Gerencia, el CISO (Revisar, actualizar y ejecutar pruebas de los planes de contingencia, continuidad y recuperación asociados a los servicios de TI; Monitorizar los planes de continuidad de servicios y planes de recuperación de TI; Establecer y cumplir con el plan de acciones correctivas y de mejora continua que propendan de la continuidad del negocio), el DAFP (Analizar las acciones disciplinarias a tomar en caso de presentarse incumplimiento por parte de los servidores públicos pertenecientes al DAFP en materia de continuidad del negocio)

También se evidenció el Plan Estratégico de Seguridad de la Información – PESI V02 (febrero 2026, que contiene un eje estratégico de continuidad articulado al portafolio de proyectos de la OTIC para la vigencia 2026, el cual fue presentado ante el Comité en la Planeación Institucional de enero 2026 (evidenciado en la Plantilla Comité Planes 2026 – enero 2026).

Respecto a la política mencionada, la OTIC en la ruta \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\ Plan Estratégico de Seguridad de la Información, desarrolló el borrador de la actualización del documento "Política General de Seguridad de la Información"- PGSI, la cual se encuentra pendiente de su socialización y publicación. A su vez, verificando que controles de gestión se tienen para el desarrollo de esta actividad, se observó que, si bien se tiene internamente dentro de un archivo Excel la actividad relacionada con la

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)

actualización de la documentación asociada a la política de seguridad de la información, esta actividad no aparece como entregable dentro de la planeación institucional.

1.3.2. Hito 2: Actualización del Análisis de Impacto en el Negocio (BIA).

Actualmente, se puede observar en la documentación interna (Ruta: \\\\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan Estratégico de Continuidad del Negocio), el documento ya conocido de Análisis de Impacto al Negocio, versión 1 de abril 2024. Al respecto, la OTIC a hoy ya clasifico los procesos por criticidad, definió los RTO (Tiempo de recuperación objetivo) y RPO (Punto de recuperación objetivo) actuales y se identificaron herramientas tecnológicas misionales, con el fin de proceder a actualizar el documento mencionado.

Control de gestión sobre las actividades/hitos:

Verificando si esta actividad del PECN y sus hitos está inmersa en algún entregable de la Planeación Institucional gestionada en el SIGP, se pudo observar que no se tiene registrado un entregable.

Recomendaciones

1. Se debe publicar en el SIGP en el proceso de Gestion de las tecnologías de la información y socializar a los steakholders respectivos, la última versión de la “Política General de Seguridad de la Información” que ya fue debidamente actualizada. Además, se debe tener en cuenta la correlación que la temática de este documento pueda tener con el Manual de políticas de seguridad de la información y que pueda influir en la política.

   Tener siempre en cuenta como base conceptual y metodológica para la actualización de este tipo de documentación las mejores prácticas establecidas en la Guía 10 del Modelo de Seguridad y Privacidad de las Información - MSPI para la preparación de las TIC para la continuidad del negocio, establecida por MinTIC.

2. Con la información ya identificada proceder a la actualización y socialización a los responsables respectivos del Análisis de Impacto del Negocio – BIA, manteniendo el debido soporte y versionamiento a nivel interno en la carpeta YAKSA correspondiente.

3. Con el fin de mantener la trazabilidad y control en la gestión de las actividades inmersas en el PECN, se recomienda crear un entregable y sus respectivas actividades en la Planeación Institucional del SGI, relacionado con esta actividad.

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)

1.4. Actividad 4: Diseñar y documentar el Plan de gestión del cambio documentado

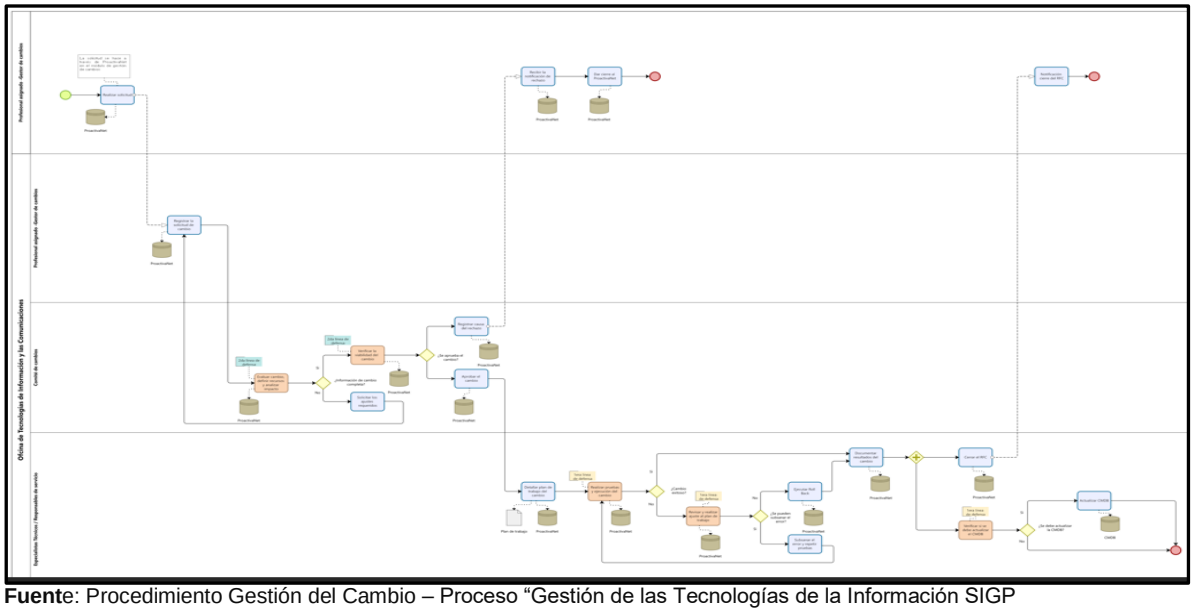
Responsables: Profesional OTIC

1.4.1. Hito 1: Plan de Gestión del Cambio de la OTIC, definiendo el procedimiento para la solicitud, evaluación, aprobación, implementación, comunicación y seguimiento de los cambios tecnológicos.

Estado actual

Actualmente, la Ingeniera responsable por parte de la OTIC, está desarrollando un borrador actualizado del documento de gestión del cambio, tomando como base el documento inicialmente publicado en el SIPG denominado “Lineamientos para la Gestión de Cambios de Tecnologías de la Información “, versión 2 de enero 2025. Documento que fija como alcance la realización de la gestión de los cambios que incluyen componentes de TI de forma articulada, identificando los servicios, actividades, roles e indicadores que servirán para evaluar la efectividad del proceso de Gestión de Cambios.

A su vez para esta actividad, también la OTIC se está apalancando en el procedimiento actual de “Gestión de Cambios” (Versión 3 diciembre 2024) publicado en el SIGP, como se puede observar en el gráfico siguiente.



Fuente: Procedimiento Gestión del Cambio – Proceso “Gestión de las Tecnologías de la Información SIGP

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)

Al respecto, en la ruta: \\yaksa.dafp.local\10030OTIC\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLAN_CONTINUIDAD, se observó el documento borrador que está siendo actualizado, en cumplimiento de los lineamientos de la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas para la gestión de servicios de tecnologías de la información. Este documento posee parcialmente los siguientes elementos:

Introducción. Objetivo. Objetivos secundarios. Alcance. 1. Articulación con el Lineamiento y el Procedimiento de Gestión de Cambios. 2. Marco Normativo. 3. Principios de la gestión del cambio. 4. Definiciones. 5. Clasificación de los cambios. 5.1. Tiempos de atención por tipo de cambio. 6. Roles y responsabilidades. 6.1. Segregación de funciones. 7. Composición y funcionamiento del Comité de Cambios. 8. Relación con el Procedimiento de Gestión de Cambios. 9. Metodología de gestión del cambio. 9.1. Gestión de la Configuración 9.1.1. Conservación de evidencias 9.1.2. Separación y control de acceso entre ambientes 9.1.3. Articulación con otros procesos de gestión de TI 10. Metodología de clasificación de impacto y riesgo 11. Gestión de riesgos 12. Plan de comunicaciones 13. Seguimiento y monitoreo 13.1. Seguimiento al Procedimiento de Gestión de Cambios 14. Indicadores 15. Mejora continua 16. Anexos Bibliografía Anexos

Fuente: Documento Plan de Gestión de Cambios de TI v1 mayo 2026 - Borrador

Este Documento se encuentra en proceso de revisión interna por parte de la OTIC.

Control de gestión:

Se evidencia en la sábana de planeación institucional el entregable 520 “Estrategia de Continuidad Institucional en Función Pública implementada”, el cual ha venido siendo gestionado por el Profesional de SI, en el reporte de mayo 2026: “En el marco del avance de la estrategia de continuidad institucional, la OTIC adelanto el borrador del Plan de Gestión de Cambios de TI (versión 0.1), instrumento que establece los lineamientos, roles,

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

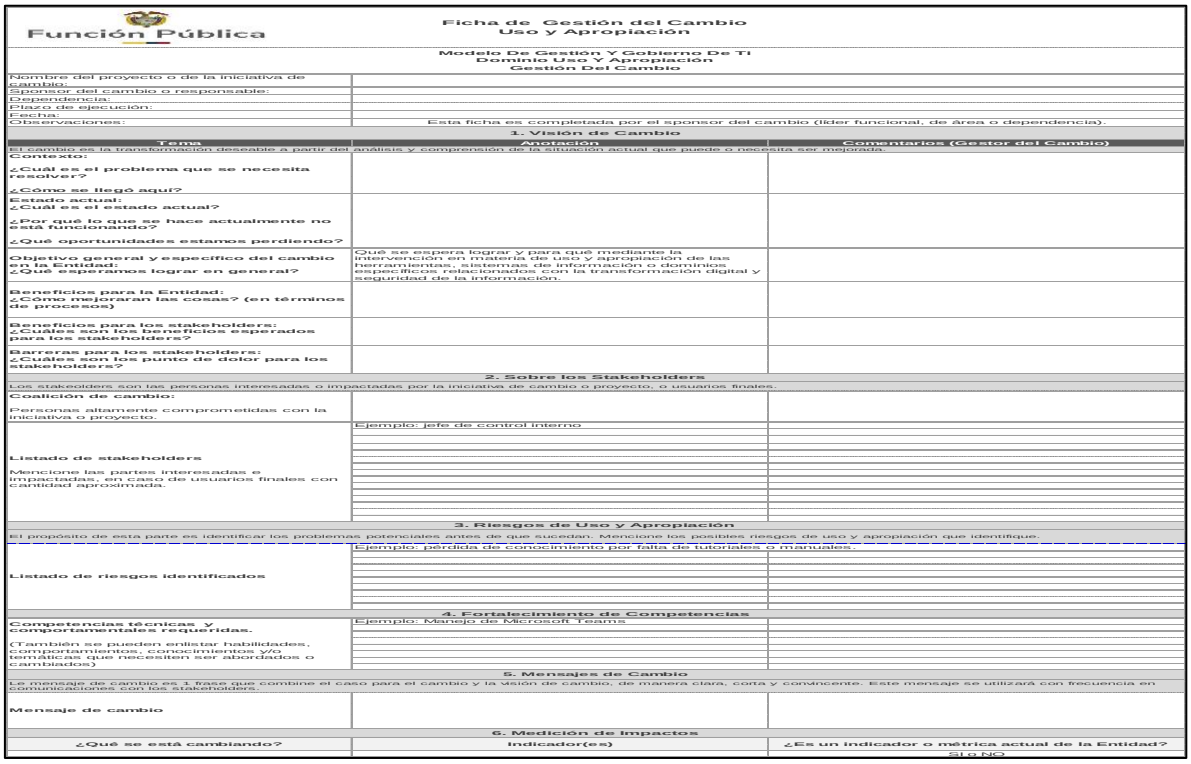
Página web:
www.funcionpublica.gov.co

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)

fases metodológicas y mecanismos de control para la gestión controlada y trazable de los cambios tecnológicos institucionales. El plan define tres tipologías de cambio estándar, normal y de emergencia, contempla una metodología estructurada en siete fases (solicitud, evaluación, aprobación, planeación, implementación, validación y cierre) e incorpora criterios de gestión del riesgo asociados a confidencialidad, integridad, disponibilidad y continuidad del negocio. Así mismo, establece indicadores de seguimiento con metas cuantificables, un plan de comunicaciones y mecanismos de mejora continua articulados con el Procedimiento de Gestión de Cambios vigente de la OTIC. Este avance contribuye directamente al fortalecimiento de las capacidades de gobierno de TI del DAFP, alineado con los lineamientos de la Política de Gobierno Digital, MIPG y el Modelo de Seguridad y Privacidad de la Información (MSPI).”

Por otro lado, también se evidencia la “Ficha de Gestión del Cambio Uso y Apropiación”, versión 3 de junio 2024 publicada en el proceso de tecnología en el SIPG, la cual deriva del Modelo de Gestión y Gobierno de TI para el Dominio de Uso y Apropiación Gestión del Cambio. En esta ficha se debe registrar por cada proyecto de TI el plan de gestión del cambio y su detalle, el cual debe relacionar los siguientes ítems:



Función Pública

Ficha de Gestión del Cambio
Uso y Apropiación

Modelo De Gestión Y Gobierno De TI
Dominio Uso Y Apropiación
Gestión Del Cambio

Nombre del proyecto o de la iniciativa de cambio:	
Sponsor del cambio o responsable:	
Dependencia:	
Plazo de ejecución:	
Fechas:	
Observaciones:	Esta ficha es completada por el sponsor del cambio (líder funcional, de área o dependencia).

1. Visión de Cambio

Tema	Anotación	Comentarios (Gestor del Cambio)
El cambio es la transformación deseable a partir del análisis y comprensión de la situación actual que puede o necesita ser mejorada.		
Contexto: **¿Cuál es el problema que se necesita resolver?** **¿Cómo se llegó aquí?**		
Estado actual: **¿Cuál es el estado actual?** **¿Por qué lo que se hace actualmente no está funcionando?** **¿Qué oportunidades estamos perdiendo?**		
Objetivo general y específico del cambio en la Entidad: **¿Qué esperamos lograr en general?**	Qué se espera lograr y para qué mediante la intervención en materia de uso y apropiación de las herramientas, sistemas de información o dominios específicos relacionados con la transformación digital y seguridad de la información.	
Beneficios para la Entidad: **¿Cómo mejorarán las cosas? (en términos de procesos)**		
Beneficios para los stakeholders: **¿Cuáles son los beneficios esperados para los stakeholders?**		
Barreras para los stakeholders: **¿Cuáles son los punto de dolor para los stakeholders?**		

2. Sobre los Stakeholders

Los stakeholders son las personas interesadas o impactadas por la iniciativa de cambio o proyecto, o usuarios finales.		
Coalición de cambio: Personas altamente comprometidas con la iniciativa o proyecto.		
Listado de stakeholders Mencione las partes interesadas e impactadas, en caso de usuarios finales con cantidad aproximada.	Ejemplo: jefe de control interno	

3. Riesgos de Uso y Apropiación

El propósito de esta parte es identificar los problemas potenciales antes de que sucedan. Mencione los posibles riesgos de uso y apropiación que identifique.		
Listado de riesgos identificados	Ejemplo: pérdida de conocimiento por falta de tutoriales o manuales.	

4. Fortalecimiento de Competencias

Competencias técnicas y comportamentales requeridas. (También se pueden enlistar habilidades, comportamientos, conocimientos y/o temáticas que necesiten ser abordados o cambiados)	Ejemplo: Manejo de Microsoft Teams	

5. Mensajes de Cambio

Le mensaje de cambio es 1 frase que combine el caso para el cambio y la visión de cambio, de manera clara, corta y convincente. Este mensaje se utilizará con frecuencia en comunicaciones con los stakeholders.		
Mensaje de cambio		

6. Medición de Impactos

¿Qué se está cambiando?	Indicador(es)	¿Es un indicador o métrica actual de la Entidad? SI o NO

Fuente: Ficha de Gestión del Cambio Uso y Apropiación – SIGP

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)

Recomendación

Mantener la continuidad en la actualización del Plan de Gestión del Cambio de la OTIC, definiendo el procedimiento para la solicitud, evaluación, aprobación, implementación, comunicación y seguimiento de los cambios tecnológico, como lo especifica el Hito. Efectuando el debido registro de gestión del entregable en la sábana de la planeación institucional, como se ha venido haciendo.

Respecto a la ficha de Gestión del Cambio Uso y Apropiación, publicada en el SIGP, analizar su posible actualización y articulación con el plan de gestión de cambios.

1.5. Actividad 5: Actualizar los Planes de recuperación de los Sistemas de Información y Aplicativos Críticos.

Responsables: Grupo de S.I - Oficial de seguridad

1.5.1. Hito 1: Elaboración y actualización de planes de continuidad y recuperación

Los planes de recuperación DRP para los sistemas misionales y algunos de apoyo se mantienen en las mismas versiones de años anteriores. Estos DRPs aún no han sido actualizados.

A continuación, se despliega un cuadro resumen del estado actual por versión y fecha de los DRPs existentes:

Sistema	Versión	Fecha	Ruta
SUIT	Ver 3	may-25	\\yaksa\1030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS\Plan_recupera_sistemas_informacion
FURAG	Ver 5	jun-25	
SIGEP II	Ver 2	dic-24	
Kactus	Ver 1	ago-24	
Aplicativo por la integridad	Ver 1	ago-24	
Orfeo	Ver 1	Dic-24	

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

Se presenta enseguida un resumen de los aspectos más importantes encontrados en cada DRP:

Sistemas Misionales

FURAG

Objetivo: Establecer el plan de recuperación para el Sistema FURAG en caso de una falla que genere una indisponibilidad del sistema por un tiempo mayor al establecido en el acuerdo de nivel de servicio ANS, dando continuidad y recuperar el servicio por inconvenientes en la infraestructura tecnológica de FURAG.

Se consideraron los siguientes aspectos en el plan:

- Condiciones generales
  - ✓ Metodología
  - ✓ Plan de trabajo ante la falla
- Fase 1 Planear
  - ✓ Plan de Continuidad de Función Pública
  - ✓ Plan de Recuperación para el Formulario Único Reporte de Avances de la Gestión-FURAG
  - ✓ Infraestructura ambiente de producción
  - ✓ Infraestructura Ambiente de Preproducción (Azure)
  - ✓ Infraestructura alterna - ambiente de preproducción (Onpremise)
  - ✓ Vista Lógica
  - ✓ Plan alterno manual implementado por el dueño del servicio o sistema.
  - ✓ Tratamiento y gestión de usuarios (Entidades)
- Fase 2: Hacer
  - ✓ Acciones de Prevención
  - ✓ Roles y Responsabilidades Ambiente Producción
  - ✓ Planes de recuperación requeridos
  - ✓ Recuperación del sistema
  - ✓ Riesgos y Vulnerabilidades.
- Verificar y mejora continua
  - ✓ Desarrollo de las Pruebas

SIGEP

Objetivo: Establecer el plan de recuperación para el Sistema SIGEP II en caso de una falla que genere una indisponibilidad del sistema ante la eventualidad de incidentes, accidentes y/o estados de emergencias.

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)

Se consideraron los siguientes aspectos en el plan:

- Condiciones generales:
  - ✓ Metodología
- Fase 1. Planear
  - ✓ Plan de recuperación para el sistema de información SIGEP II
  - ✓ Identificación de la Infraestructura
  - ✓ Servidores
  - ✓ Bases de datos
  - ✓ Software base del diseño de arquitectura del sistema de información
  - ✓ Estrategia de Recuperación
- Fase 2: Hacer
  - ✓ Roles y Responsabilidades
  - ✓ Políticas de respaldo, custodia y recuperación de la información
  - ✓ Riesgos y Vulnerabilidades
  - ✓ Actividades del Plan de Recuperación para Sigep
  - ✓ Activación y Notificación
- Fase 3 y 4. Verificar y mejora continua

SUIT

Objetivo: Establecer el plan de recuperación para el Sistema SUIT en caso de una falla que genere una indisponibilidad del sistema por un tiempo mayor al establecido.

Se consideraron los siguientes aspectos en el plan:

- Metodología
- Fase 1: Planear
  - ✓ Plan de Continuidad de Función Pública
  - ✓ Plan de Recuperación para el Sistema de Información SUIT
  - ✓ Descripción del Estado Actual del Sistema de Información SUIT
  - ✓ Identificación de la Infraestructura
  - ✓ Servidores
  - ✓ Bases de Datos
  - ✓ Software Base del Diseño de Arquitectura del Sistema de Información
  - ✓ Estrategia Recuperación
- Fase 2: Hacer
  - ✓ Roles y Responsabilidades
  - ✓ Políticas de Respaldo, Custodia y Recuperación de la Información
  - ✓ Tiempos RPO y RTO
  - ✓ RTO (Recovery Point Objective)

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)

  - ✓ RTO (Recovery Time Objective)
  - ✓ Proceso de Restauración
  - ✓ Riesgos y Vulnerabilidades
  - ✓ Actividades del Plan de Recuperación para SUIT
  - ✓ La Activación y Notificación
  - ✓ Fase de Recuperación
  - ✓ Fase de Restauración del Servicio
- Fase 3 y 4: Verificar y Mejora Continua
- Anexos
  - ✓ Anexo 1. Plan de Pruebas Plan de Recuperación de SUIT
  - ✓ Anexo 2 Registro de Pruebas
  - ✓ Desarrollo de las Pruebas

APLICATIVO POR LA INTEGRIDAD

Objetivo**:** Establecer el plan de recuperación para el Sistema APLICATIVO POR LA INTEGRIDAD en caso de una falla que genere una indisponibilidad del sistema por un tiempo mayor al establecido en el Acuerdo de Nivel de Servicio (ANS). Dando continuidad y recuperar el servicio por inconvenientes en la infraestructura tecnológica de APLICATIVO POR LA INTEGRIDAD.

Se consideraron los siguientes aspectos en el plan:

-
- Condiciones generales
  - ✓ Metodología
  - ✓ Plan De Continuidad de Función Pública
- Fase 1. Planear
  - ✓ Plan de Recuperación para El Sistema de Información Aplicativo por la Integridad
- Fase 2: hacer
  - ✓ Acciones de prevención
  - ✓ Roles y responsabilidades
  - ✓ Planes de recuperación requeridos
  - ✓ Políticas de respaldo, custodia y recuperación de la información
  - ✓ Actividades del plan de recuperación para aplicativo por la integridad
  - ✓ Activación y notificación
  - ✓ Plan de recuperación
  - ✓ Mecanismos de seguimiento
  - ✓ Desactivación de la contingencia
- Fase 3 y 4. Verificar y mejora continua
  - ✓ Mejora continua
  - ✓ Contingencia sin sistema
  - ✓ Posibles Vulnerabilidades

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)

- ✓ Posibles Amenazas
- ✓ Posibles Riesgos

Sistemas de Apoyo

KACTUS

Objetivo: Recuperar el servicio de KACTUS por daño físico, daño en la aplicación o inconvenientes en la infraestructura tecnológica.

Se consideraron los siguientes aspectos en el plan:

- Condiciones Generales
- Infraestructura
- Actividades
- Cuadro Responsables
- Planes de Recuperación Requeridos
- Contingencia sin sistema GGH
- Posibles Vulnerabilidades
- Posibles Amenazas – Centro de datos de Función Pública
- Posibles Riesgos
- Posibles Controles
- Plan de recuperación ante desastres (Disaster Recovery Plan o DRP)
- Identificación del problema
- Proceso de restauración del servidor de aplicaciones
- Instalación de motor Oracle
- Configuración de la aplicación kactus
- Revisión y verificación
- Prueba de recorrido

ORFEO

Objetivo: Recuperar el servicio de Orfeo por daño físico, daño en la aplicación o inconvenientes en la infraestructura tecnológica.

Se consideraron los siguientes aspectos en el plan:

- Condiciones Generales
- Infraestructura

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)

- Actividades
- Cuadro Responsables
- Planes de Recuperación Requeridos
- Contingencia sin sistema
- Posibles Vulnerabilidades
- Posibles Amenazas
- Posibles Riesgos
- Posibles Controles

Como se puede observar en todos los DRP actuales, no se evidencia:

- Un estándar en la forma y contenido de los elementos clave que debe contener un plan de recuperación de desastres.
- Tiempos RTO y RPO para cada uno de los sistemas (Solo se evidencia en SUIT)
- Roles y responsabilidades asignados a cargos, se registran por persona y los contactos son los números telefónicos personales.
- Para los sistemas de apoyo Kactus y Orfeo Procedimientos definidos de respaldo, recuperación y ejecución de pruebas reales y de recorrido.

1.5.2. Hito 2: Asignación de roles y responsabilidades para la recuperación

Este hito está siendo gestionado al interior de cada DRP, como se puede ver en el hito anterior. Al respecto, se pudo observar al interior de cada DRP que los roles y responsabilidades estan siendo asignados directamente a nivel de persona, con sus respectivos datos de contacto personal, algunos de estos contactos ya no laboran en la Entidad. Tampoco se evidencia la inclusión de los responsables operativos (Dependencias misionales).

Hito 3: Realizar y documentar ejercicios de pruebas de recuperación ante el desastre tecnológico según capacidades y periodicidad establecidas.

Según lo aseverado por el Profesional de Seguridad de la Información, para la presente vigencia no se han efectuado pruebas de recorrido e integrales de los DRP. Por ende, no se evidencian cronogramas y/o plan de ejecución, informes, bitácoras y fichas técnico/operativas de las pruebas de los DRP de sistemas misionales o de servicios de apoyo durante la vigencia.

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)

Teniendo en cuenta la respuesta de la OTIC, al informe preliminar mediante correo electrónico del 12/08/2026 firmado por la Ingeniera Marcela Ramos, al respecto, esta oficina pudo evidenciar que la ejecución de pruebas integrales de DRP demanda no solo disponibilidad del equipo técnico de la OTIC, sino también ventanas de mantenimiento coordinadas con las Dependencias funcionales usuarias de cada sistema, infraestructura de contingencia disponible y, en algunos casos, participación del proveedor externo. Estos requerimientos, combinados con las limitaciones de capacidad presupuestal, técnica y de recurso humano del área, han sido la principal razón por la que históricamente las pruebas no se han ejecutado con la periodicidad recomendada.

Por otro lado, el Diagnóstico de Seguridad y Privacidad de la Información V01 (marzo 2026), evalúa la postura de ciberseguridad institucional bajo la norma ISO 27001:2022 Anexo A y el framework NIST CSF, proveyendo la línea base técnica para las acciones de mejora de los DRPs. Identifica el dominio de Controles Tecnológicos (A.8) con una efectividad del 58%, lo que es consistente con las brechas señaladas por la OCI y refuerza la necesidad de los recursos adicionales señalados.

Según lo documentado en algunos planes de recuperación se efectuaron en vigencias anteriores ejercicios tangenciales relacionados con:

- Ejecución de pruebas de restauración de bases de datos (Oracle database)
- Pruebas de recorrido (Kactus)
- Desarrollo de actividades de mejora en SIGEP II que hacen parte de las pruebas del plan de continuidad (Bases de datos, publicación de nuevas versiones tanto en ambiente de producción como de capacitación de servidores de aplicación y backend, componente de hadoop)

Finalmente, no se evidencia un cronograma o plan de ejecución de las pruebas de los DRP de sistemas misionales o de servicios de apoyo durante la vigencia.

Control de gestión

Al respecto, se tiene registrado en la planeación institucional el entregable “Estrategia de Continuidad Institucional en Función Pública implementada”, la cual orienta las siguientes actividades:

- Actualizar los Planes de recuperación de los Sistemas de Información y Aplicativos Críticos: En esta actividad, se evidencia el respectivo avance de los meses de febrero

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)

y mayo, donde se especifica por parte del responsable la necesidad de actualizar la documentación técnica y operativa de los sistemas de información FURAG, SUIT y SIGEP. Esta es prioritaria debido a los cambios y ajustes técnicos implementados recientemente en dichos sistemas, los cuales deben quedar reflejados en los planes de continuidad para garantizar su efectividad ante cualquier eventualidad. Con el fin de dar cumplimiento al cronograma de seguimiento institucional, se solicitó el envío de la siguiente manera:

- ✓ Reportes de avance: Se deberán remitir entregables parciales durante los meses de mayo y septiembre.
- ✓ Entrega final: El documento actualizado y validado deberá ser enviado a más tardar en el mes de octubre."

- Realizar y documentar ejercicios de pruebas de recuperación ante el desastre tecnológico según capacidades y periodicidad establecidas: Aún no se registrado avance de la actividad.

Recomendaciones

1. Se deben actualizar todos los DRPs de los sistemas misionales y de apoyo existentes teniendo en cuenta entre otros los siguientes aspectos:

   - ✓ Estandarizar el formato y contenido inmerso en cada DRP. Todos los planes deben tener la misma estructura a nivel procedimental.
   - ✓ Ajustar los roles y responsabilidades de cada plan, teniendo en cuenta los cargos de los responsables; la inclusión de los responsables no solo técnicos sino de las dependencias funcionales que intervienen en la operación del plan; la asignación y registro de números de contacto corporativos, no personales.
   - ✓ Definición de tiempos de RTO y RPO para cada sistema misional y de apoyo .
   - ✓ Procedimientos definidos de respaldo, recuperación y ejecución de pruebas integrales y de recorrido para Kactus y Orfeo.

2. Socializar a los responsables y publicar en el SIGP con el apoyo de la Oficina Asesora de Planeación cada uno de los DRPs actualizados, manteniendo la periodicidad respectiva en este proceso y el control de versionamiento correspondiente.

3. El CISO o responsable asignado para efectuar el seguimiento al PECN, debe conocer y mantener el acervo de soportes de todas las pruebas a todos los DRPs efectuadas

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)

durante cada vigencia (Cronogramas de prueba, fichas técnicas y/o informes de resultados de la ejecución).

4. De acuerdo con lo establecido en Plan de recuperación ante desastres tecnológicos, en el numeral “13. Estrategia de pruebas al DRP”, en la preparación de la prueba se debe “*Definir el cronograma y el tiempo en las que se ejecutarán las pruebas*”, por ende, en cada vigencia se debe definir dicho cronograma, teniendo en cuenta el equipo de recuperación ante desastres y el equipo de apoyo administrativo requerido, la disponibilidad de los recursos y las fechas de ejecución, entre otros.

5. Como se ha venido recomendando en seguimientos de vigencias anteriores, la OTIC en Coordinación con la Dirección Técnica o Dependencia correspondiente, y bajo los recursos financieros, operativos y de infraestructura requeridos, deben programar mínimo una prueba de cada DRP de los sistemas misionales y de apoyo una vez al año. Se recuerda que las pruebas sirven para verificar su efectividad, garantizar que los sistemas se puedan restaurar correctamente y asegurar que el recurso humano responsable sepa cómo actuar. Además, las pruebas permiten identificar y corregir fallas antes de que ocurra un incidente real, minimizando así la pérdida de datos, el tiempo de inactividad y los costos de recuperación, además de asegurar el cumplimiento normativo (Protección de datos y continuidad del negocio, entre otras).

6. Complementar los DRPs actuales con fichas técnicas más estructuradas y estandarizadas a ser utilizadas para el registro y soporte de las pruebas. Se recomienda considerar hasta donde aplique la siguiente información en cada ficha:

   - Generalidades del ejercicio:

     - Objetivos: Qué se espera lograr con el ejercicio (p. ej., probar un protocolo específico, evaluar la competencia del equipo).
     - Alcance: Los procesos, departamentos o sistemas que se incluirán en el ejercicio.
     - Escenario: Una descripción detallada del evento simulado (p. ej., ciberataque, fallo de sistema, desastre natural) y cómo afectará a las operaciones.

   - Roles y responsabilidades:

     - Equipo de respuesta: Quiénes forman parte del equipo de respuesta y cuál es su función específica durante el ejercicio.

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)

- Líderes de equipo: Información de contacto y responsabilidades de los líderes de cada área.
- Portavoces: Quién está autorizado para comunicarse con los medios u otras partes interesadas externas.

➢ Procedimientos de respuesta y recuperación

- Protocolos de comunicación: Cómo se comunicará la empresa internamente durante la crisis.
- Procedimientos de emergencia: Pasos a seguir para la respuesta inmediata al evento simulado.
- Estrategias de recuperación: Los pasos específicos para restaurar los servicios y operaciones críticas.
- Objetivos de tiempo de recuperación (RTO): El tiempo máximo permitido para que cada función crítica esté inactiva antes de que ocurra un daño significativo.

➢ Recursos críticos

- Personal: Información del personal clave, incluidos sus roles y datos de contacto.
- Sistemas e infraestructura: Una lista de los sistemas, aplicaciones, bases de datos, hardware y su infraestructura crítica, junto con los planes de respaldo.
- Proveedores y socios: Lista de proveedores clave, contactos y detalles de los acuerdos de servicio (contratos, garantías, etc.).

➢ Análisis y seguimiento

- Resultados: Un registro de lo que ocurrió durante el ejercicio, los problemas encontrados y las soluciones aplicadas.
- Lecciones aprendidas: Un análisis de las fortalezas y debilidades identificadas durante la simulación.
- Plan de mejora: Un resumen de las acciones correctivas que se tomarán para mejorar el plan de continuidad de negocio.

7. Una vez se tengan definidas y estandarizadas las fichas técnicas para ejercicios de prueba, aplicarlas en cada prueba de los DRP registrando la información de todos los resultados. Importante mantener el acervo de soportes en una ruta del servidor de carpetas compartidas YAKSA.

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)

Conclusiones y Recomendaciones Generales

1. Se denota a nivel general el compromiso de la OTIC, quienes bajo la limitación presupuestal y de talento humano especializado que ha afectado de manera sostenida a la dependencia y a nivel transversal en su gestión durante los últimos años, ha venido gestionando hasta donde es posible el PECN. Situación soportada en el Plan estratégico de Seguridad de la Información – PESI v2 2026, el informe de Seguimiento MSPI – OCI (septiembre 2025) y en Proyecto de Inversión 20230000000140 (vigencia 2024-2027. Por ende, esta Oficina como lo ha venido expresando en vigencias anteriores, recomienda a la Alta Dirección considerar y propender por mantener y aumentar el recurso financiero y humano necesario a nivel estratégico y de toma de decisiones.

2. Con el fin de mantener la trazabilidad y control de la gestión del Plan Estratégico de Continuidad del Negocio - PECN, se deben incorporar todos los hitos/actividades determinadas en los entregables de dicho plan, en el módulo de planeación institucional del SGI. Esto con el fin de mantener la debida trazabilidad y soporte a la gestión desarrollada por el(los) responsable(s).

3. Con el apoyo de la OAP, la OTIC debe revisar y estandarizar la estructuración de forma de los documentos de los DRPs oficializados y publicados en el SIPG, en el proceso de “Gestión de las Tecnologías de la información”. Lo anterior debido a que se evidenciaron índices de contenido y estructuras diferentes entre algunos documentos.

4. Efectuar periódicamente el seguimiento al estado de actualización del escenario de análisis de impacto - BIA, el cual brinda la descripción detallada de los pasos que se llevan a cabo para documentar el análisis de impacto al negocio, entendiendo su importancia para la fundamentación del Plan de Continuidad del Negocio y para la estructuración, diseño y realización de pruebas de la recuperación ante el desastre. Incluir este seguimiento como actividad en el PECN para la siguiente vigencia.

5. Bajo la premisa de mantener en la entidad un presupuesto asignado a la infraestructura técnica y operativa y de talento humano requerido para los ejercicios de prueba integral de los DRPs, se deben adelantar ejercicios periódicos de las pruebas mencionadas sobre la efectividad de todos los DRPs oficialmente establecidos. Manteniendo además todo el acervo de soportes que involucra la gestión de la planeación, ejecución., resultados y retroalimentación (Mejora continua) de cada prueba.

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)

6. Se recomienda previo análisis tener en cuenta la implementación en el corto o mediano plazo de las recomendaciones detalladas en cada una de las actividades inmersas en el PECN, registradas a lo largo del presente informe.

Jorge Iván De Castro Barón

Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2026.08.13 11:15:32 -05'00'

Jorge Iván De Castro Barón
Jefe Oficina de Control Interno

Elaboro: Juan Mauricio Cornejo – contratista OCI

INFORME DE SEGUIMIENTO AL PLAN ESTRATÉGICO DE CONTINUIDAD DEL NEGOCIO

Versión 01
Evaluación Independiente
Agosto 2026

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)