Función Pública

INFORME DE SEGUIMIENTO AL PLAN ESTRATÉGICO DE CONTINUIDAD DEL NEGOCIO

Evaluación Independiente

OFICINA CONTROL INTERNO

Versión 01

Octubre de 2025

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 2025 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 2025, el cual busca "*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 registradas en el plan publicado en la sección de transparencia de la página WEB de Función Pública son:

- Establecer las bases de datos y sistemas misionales de la Entidad.
- Establecer los requerimientos legales, normativos y de cumplimiento para la prestación de los servicios de Tecnologías de la Información.
- Actualizar 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 Pública.
- Planificar y llevar a cabo el assessment 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

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 2025.

1.1. Actividad 1: Establecer las bases de datos y sistemas misionales de la entidad.

Responsables: Oficina de Tecnologías de la Información y las Comunicaciones- OTIC
Oficina Asesora de Planeación- OAP.

1.1.1. Hito1: Matriz de riesgos que afecten la disponibilidad de los servicios misionales actualizada.

Estado Actual:

Se evidencia en la matriz de riesgos actual registrada en el Sistema de Gestión Integral - SGI, los siguientes riesgos orientados a la disponibilidad de los sistemas o servicios de información:

- ✓ Código 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 contro*l", proceso TI.

- ✓ Código 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.

- ✓ Código 112 (Aprobado), "*Posibilidad de afectación reputacional por violación de la reserva, disponibilidad, confidencialidad o integridad en la información, debido a la ausencia o débil parametrización de permisos de acceso en los repositorios documentales o de la documentación generada por el Proceso*". Proceso Control Disciplinario Interno.

Por otra parte, al interior de la entidad se evidencia el "Plan de Tratamiento de Riesgos de Seguridad 2025" Versión 1 - enero 2025", el cual está publicado en la Página web del DAPF y tiene por objetivo: "Identificar, evaluar y mitigar los riesgos relacionados con la seguridad

de la información y los activos de la entidad. abordando diversos aspectos para garantizar la integridad, confidencialidad y disponibilidad de la información, entre ellos la *revisión de los planes de recuperación de servicios de Tecnología de Información*; siguiendo además las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016). Garantizando que los riesgos asociados con la seguridad de la información y los activos de la organización estén adecuadamente gestionados, para minimizar el impacto de eventos negativos"; en dicho plan se tienen especificadas las siguientes actividades:

Plan de Tratamiento de Riesgos de Seguridad 2025
Versión 1 - Enero 2025

Objetivo: identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información y los activos de la entidad. abordando diversos aspectos para garantizar la integridad, confidencialidad y disponibilidad de la información, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016). Garantizando que los riesgos asociados con la seguridad de la información y los activos de la organización estén adecuadamente gestionados, para minimizar el impacto de eventos negativos.

No.	Actividades	Meta	indicador	Fecha Inicio	Fecha Fin
1	Identificar y analizar las amenazas actuales y potenciales que podrían afectar la seguridad de los activos	Realizar un Análisis de Amenazas y sus posibles soluciones	número de amenazas atendidas VS número de amenazas reportadas	1/02/2025	20/06/2025
2	Monitorear los mantenimientos programados de la infraestructura de la entidad	realizar los mantenimientos preventivos de los servicios de infraestructura identificados	números de mantenimientos realizados VS números de mantenimientos planeados	1/04/2025	20/10/2025
3	Revisión sobre usuarios, roles y privilegios en los sistemas de información	Depuración de los usuarios, roles y privilegios en los sistemas de información	dos (2) revisiones de los planes al año	1/02/2025	30/10/2025
4	Revisar los planes de recuperación de servicios de T.I	Actualización de los planes de recuperación	dos (2) revisiones de los planes al año	3/02/2025	30/11/2025
5	Implementar programas de concientización y formación en seguridad para el personal, con el objetivo de crear una cultura de	Realizar dos campañas de concientización y Capacitación a todos los empleados de la entidad sobre formación de seguridad	número de campañas realizadas VS número de campañas planificadas	1/02/2025	30/11/2025

Fuente: Plan de Tratamiento de Riesgos de Seguridad 2025 Versión 1 - enero 2025

Actualmente, la especialista de Seguridad de la Información -SI maneja un control interno de gestión en Excel de cada actividad del plan (Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\ SEGURIDAD\REPORTE_SGI), el cual contiene la siguiente información: Entregable/nombre/riesgo, Control, Mes de reporte, Reporte, Ruta de evidencia, Nombre de archivo, indicadores.

Recomendaciones

1. Tener en cuenta la mejor práctica establecida en la Guía 10 para la preparación de las TIC para la continuidad del negocio generada por el MinTIC, con el fin de enriquecer la metodología de continuidad, en los siguientes aspectos:

   ✓ Identificación de las aplicaciones y las plataformas críticas para la operación del negocio.

- ✓ Identificación de los riesgos presentes para la continuidad (Gestión de riesgo, clasificación de los escenarios de riesgo, metodología de riesgos (Amenazas/Vulnerabilidades).

2. El (Los) responsable(s) asignado(s) para la gestión del PECN, debe(n) como segunda línea de defensa monitorear periódicamente la gestión del tratamiento de riesgos de Seguridad Digital en la entidad y mantener al proceso respectivo informando sobre su evolución.

1.1.2. Hito 2: Listado de bases de datos y sistemas misionales documentada.

Estado actual:

Antecedente: el profesional de seguridad de la OTIC con el apoyo de la OAP y el Grupo de Gestión Administrativa, de acuerdo con la plantilla sugerida por MinTIC, actualizó el archivo de inventario de activos de información, el cual reposa en la Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS APOYO\ SEGURIDAD\PLANES POLITICAS\PLAN ESTRATEGICO SEGURIDAD.

Verificando el inventario de activos mencionado, se pudieron evidenciar las veintinueve (29) bases de datos de la Entidad debidamente registradas, las cuales se mencionan a continuación:

- ✓ Kactus
- ✓ Kactus-Pruebas
- ✓ Orfeo
- ✓ Orfeo-Desarrollo
- ✓ Proactivanet
- ✓ Proactivanet - Pruebas
- ✓ Servidor De Antivirus
- ✓ Servidor De Antivirus
- ✓ Oda Nodo 1
- ✓ Oda Nodo 2
- ✓ Oda Nodo 1
- ✓ Oda Nodo 2
- ✓ Herramienta Veedurías - Base De Datos
- ✓ Oda X7-2-Ha
- ✓ Oda X7-2-Ha
- ✓ Oracle Database Standard Edition - Processor Perpetual
- ✓ Oracle Database Standard Edition One - Processor Perpetual

- ✓ Oracle Weblogic Suite - Processor Perpetual
- ✓ Oracle Weblogic Suite - Named User Plus Perpetual
- ✓ Oracle Weblogic Suite - Processor Perpetual
- ✓ Oracle Real Application Clusters - Processor Perpetual
- ✓ Oracle Directory Services Plus - Processor Perpetual
- ✓ Oracle Database Enterprise Edition - Processor Perpetual
- ✓ Oracle Database Enterprise
- ✓ Oracle Real Application Clusters-Processor Perpetual
- ✓ Oracle Database Enterprise Edition - Processor Perpetual
- ✓ Oracle Database Enterprise
- ✓ Oracle Database Standard Edition - Named User Single Server
- ✓ Oracle Database Standard Edition - Named User Single Server

Respecto a los sistemas misionales, se puede apreciar en la Base de Datos de Gestión de la Configuración (CMDB) de la entidad, registrada en la herramienta de Mesa de Ayuda Proactivanet, cada sistema misional o de apoyo que esta implementado en la Entidad, con su correspondiente información detallada sobre los componentes de la infraestructura de TI y sus relaciones. A continuación, se muestran los aplicativos o herramientas contenidas:

- ✓ Acceso a Internet
- ✓ Antivirus
- ✓ Aplicativo por la Integridad Pública
- ✓ BACKUP
- ✓ Banco de Éxitos
- ✓ Correo Electrónico Office 365
- ✓ Directorio Activo
- ✓ EVALUACION JEFES CONTROL INTERNO
- ✓ FURAG
- ✓ FURAG III
- ✓ GESTOR NORMATIVO
- ✓ Hadoop
- ✓ Mesa de Servicio
- ✓ Nomina Kactus
- ✓ ODAX7-MASTER-SCAN
- ✓ ORFEO
- ✓ PETICIONES, QUEJAS Y RECLAMOS
- ✓ Portal Función Pública
- ✓ Servidor de Archivos
- ✓ SIGEP
- ✓ SIGEP II
- ✓ SIGEP(Capacitación)
- ✓ Sistema de Gestión Institucional (SGI)

- ✓ SUIT (Producción)
- ✓ SUIT (pruebas)
- ✓ SUIT(capacitación)
- ✓ VisualSIE

1.1.3. Hito 3: Matriz de infraestructura de soporte a bases de datos y/o aplicaciones misionales documentada.

La matriz mencionada, está soportada en el inventario de activos de información y en la CMDB como se mencionó en el punto anterior. No obstante, el auditado no tiene claridad que se pretendía cubrir por demás en este hito.

Como complemento a lo anterior, se muestra la información de registro requerida en el inventario de activos de información:

Registros	**ID**
	Serie/Subserie documental
Identificación y categorización del activo	**Proceso**
	Dependencia
	Nombre o titulo del activo
	Descripción del contenido del activo de información
Clasificación del activo	**Software**
	Hardware
	Información
Características del activo	**Medio de conservación y/o soporte**
	Formato de almacenamiento
	Idioma
	Disponibilidad de la información del activo
Ubicación del activo o lugar de consulta	**Tipo de ubicación**
	El activo está a cargo de un tercero o proveedor
	Electrónica /Digital
Ciclo de vida del activo	**Fecha de generación o adquisición**
	Estado
Responsabilidades de acceso, custodia y soporte al activo de información	**Usuarios**
	Custodio
	Responsable técnico
Calificación del activo	**El activo es crítico para las operaciones Internas del negocio**
	El activo es crítico para el servicio externo (grupos de valor) o del negocio
	Clasificación de la información Ley 1712 de 2014
	Clasificación de la información Ley 1581 de 2012 y Ley 1266 de 2008 (Habeas Data) sólo aplica para datos personales
Valoración del activo	**Confidencialidad**
	Integridad o Completitud
	Disponibilidad
	Valoración del activo
	Valoración acumulativa

Fuente: Archivo de inventario “2025-07-31_Formato_inventario_activos_mostrar.xls”

Recomendación

Analizar si la información contenida en los dos registros (CMDB e Inventario de activos de información) da suficiencia al punto. Para la siguiente vigencia analizar se es necesario unificar el hito dos (2) con el tres (3).

1.2. Actividad 2: Establecer los requerimientos legales, normativos y de cumplimiento para la prestación de los servicios de Tecnologías de la Información.

Responsables: OTIC

1.2.1. Hito 1: Acuerdo de niveles de prestación de los servicios de tecnologías de la información – TI actualizados en ProactivaNet

Los 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:

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 octubre 2025

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).

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

Responsables: OTIC, OAP.

1.3.1. Hito 1: Documento técnico del sistema de continuidad actualizado.

Estado actual:

El Documento técnico del Sistema de continuidad era un documento que había sido trabajado en la vigencia 2023 por el CISO de la OAP bajo las mejores prácticas y que se encontraba en proceso de revisión en su momento (Documento: "2023-01-25_Anexo_Documento_tecnico_plan_continuidad_negocio.pdf" / ruta: \\yaksa.dafp.local\10020OAP\2023\TRD\PLANES\ESTRATEGICO_INSTITUCIONAL\CONTINUIDAD_NEGOCIO).

Este documento técnico, se encuentra estructurado bajo las mejores prácticas y marco legal (Ley 1523 de 2012, Decreto 1078 de 2015, Ley 1955 de 2018, Política nacional de gestión del riesgo de desastres y las obligaciones en materia de Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) del decreto 1072 de 2015, Modelo Integrado de planeación y gestión, 3ª. Dimensión, Política de gobierno digital, Política Nacional de Seguridad Digital - Documento CONPES 3854 de 2016, entre otros) y tiene por objetivo "*Definir las actividades detectivas, preventivas, reactivas y correctivas para gestionar adecuadamente las situaciones que sean calificadas como emergencia y puedan comprometer la seguridad del personal, la prestación de servicio o la continuidad de las funciones misionales*".

No obstante, en la actualidad, dicho documento no se ha sido actualizado, publicado y socializado.

Por otro lado, se encuentra publicado el plan de recuperación ante desastres tecnológicos, generado por la OTIC, publicado en el Sistema Integrado de Planeación y Gestión - SIPG, con versión 5 de diciembre 2024, este plan tiene por objetivo *"Diseñar y actualizar periódicamente el plan de recuperación ante desastres tecnológicos - DRP de Función Pública, para actuar adecuadamente ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente.*". Este documento determina el desarrollo de las estrategias en la recuperación y continuidad de los sistemas de información y la infraestructura tecnológica que la soporta, contra posibles desastres de diferente naturaleza que afecten los procesos misionales e institucionales de la entidad, tanto externos como

internos y así, estar preparados para cualquier eventualidad y en el menor tiempo posible restablecer los servicios digitales y disminuir la pérdida de los recursos tecnológicos.
Al respecto, no se evidencia en el plan en el numeral “10. Procedimientos de recuperación de cada sistema”, la inclusión del procedimiento para la herramienta ORFEO, sobre el cual existe su correspondiente DRP.

Recomendaciones

1. Tal y como se había recomendado en el seguimiento al PECN efectuado en la vigencia 2024 por esta Oficina, “Se debe actualizar, publicar y socializar la última versión del Documento Técnico del Plan de Continuidad del Negocio en la página web del DAFP”. Además, se debe tener en cuenta la correlación que la temática de este documento pueda tener con el plan de recuperación ante desastres tecnológicos generado por la OTIC y que pueda influir en una posible actualización de dicho plan.

   Tener en cuenta para la actualización de estos documentos 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. Actualizar el plan de recuperación ante desastres tecnológicos con la inclusión del procedimiento de recuperación del gestor de correspondencia y PQRSDs ORFEO.

1.3.2. Hito 2: Matriz de escalamiento de funcionarios que deben intervenir en el caso de interrupción documentada e integrada al plan de continuidad.

Las matrices de escalamiento se evidencian en el documento general del plan de recuperación ante desastres tecnológicos OTIC 2025, en el numeral 2 (Roles y responsabilidades) como se muestra a continuación:

Responsable	Rol	Actividad
Línea Estratégica	Alta dirección (director, subdirector), secretario general, jefe de OAP, jefe de OTIC) Comité Institucional de Gestión y desempeño Comité de emergencias director, subdirector, secretario general, jefe de OAP	Definir y comunicar los lineamientos generales para el establecimiento y reacción ante eventualidades que impidan la continuidad, a través del plan de continuidad y el plan de recuperación. Proveer recursos para atender las necesidades del plan de continuidad y el plan de recuperación. Tomar decisiones institucionales para la operación del plan de continuidad y del plan de recuperación ante desastres presentadas por los responsables.

Responsable	Rol	Actividad
		Citar a las personas que conformar el comité de emergencias y activar la contingencia o desastre tecnológico según la alerta.
Primera Línea	Jefe de la Oficina de las Tecnologías de la Información – Líder del proceso.	Asesorar a la alta dirección sobre eventos y controles de los riesgos de continuidad, conforme a los requerimientos técnicos y normativos vigentes. Atender con diligencia los lineamientos definidos para las diferentes etapas del plan de continuidad y el plan de recuperación ante desastres.
	Equipo de trabajo delegado de la Oficina de Tecnologías de la Información	Gestionar y ejecutar los recursos para adelantar las actividades requeridas para la activación del plan de continuidad y el plan de recuperación ante desastres. Coordinar la atención organizada y estandarizada de las actividades planificadas ante una eventualidad. Dirigir y comunicar oportunamente las situaciones de riesgo de continuidad, según los canales e instancias definidas.
Segunda Línea	Jefe de la Oficina de las Tecnologías de la Información – Líder del proceso	Asesorar a toda la entidad sobre las acciones a seguir ante un evento de riesgos de continuidad o perdida de la información ante desastres tecnológicos. Adelantar las acciones oportunas ante una eventualidad de continuidad o perdida de información ante desastres tecnológicos. Generar y activar controles para prevenir situaciones de riesgo. Documentar y conservar la trazabilidad de las acciones adelantadas.

Fuente: Numeral 2. Roles y responsabilidades (Plan de recuperación ante desastres tecnológicos OTIC 2025)

Además, en cada uno de los planes de recuperación de los sistemas misionales y los de apoyo que se encuentran implementados, se incluyen las respectivas matrices actualizadas de roles y responsabilidades.

1.3.3. Hito 3: Matriz de responsabilidades ante la disrupción actualizada y socializada.

Sobre este Hito, se evidencian los mismos soportes del hito anterior (1.3.2), no es claro cuál es la diferencia en cuanto a la matriz de roles y responsabilidades ya identificada por parte del Entidad. Lo único que no se pudo evidenciar fue su debida socialización.

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

Efectuar la debida socialización al interior del Departamento de la matriz de roles y responsabilidades identificada en el documento general del plan de recuperación ante desastres tecnológicos OTIC 2025, y mantener su actualización en el tiempo.

De otro lado, analizar la unificación de los hitos 2 y 3 de esta actividad, por cuanto su naturaleza actualmente es la misma.

1.4. Actividad 4: Documentar los ejercicios de recuperación ante el desastre.

Responsables: OTIC, OAP.

1.4.1. Hito 1: Ficha de escenarios de disrupción actualizados.

Actualmente, no se ha efectuado actualización de las fichas de escenarios de disrupción, que habían sido ya identificadas en el seguimiento de la vigencia 2024 y que tenían fecha de actualización al mes de septiembre de 2024. En dicha vigencia se encontraron desarrolladas 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.

Estas fichas se encuentran aún en la ruta: \\yaksa.dafp.local\10021GMI\2024\TRD\Originales\PLANES\SEGURIDAD_INFORMACION\Continuidad_negocio.

Recomendación

Coordinadamente la OTIC y la OAP, deben efectuar el análisis de cada ficha y determinar con el apoyo de las dependencias respectivas, si es necesaria la actualización de las acciones y responsables para la detección, activación, ejecución del plan de operación alterno y resolución del incidente.

1.4.2. Hito 2: Documento de respaldo base de datos documentado y revisado.

Se evidencia el documento de respaldo de bases de datos que se está construyendo por parte del responsable de Seguridad de la Información de la OTIC en el mes octubre de 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

presente vigencia, el cual tiene como propósito servir como guía formal y estandarizada para la realización, almacenamiento y verificación de los respaldos de la información contenida en las bases de datos institucionales. (Ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\AUDITORIA).

En él documento mencionado se detalla el paso a paso cada una de las pruebas realizadas al proceso de respaldo a las bases de datos.

Esta tarea se apoya también con la Política de Respaldo y Recuperación publicada en el SIGP, versión 6 de enero 2025. Al respecto, se evidencia una siguiente versión (7) de octubre de la presente vigencia, en proceso de socialización para próxima publicación.

Recomendación

Terminar la construcción del documento de respaldo de bases de datos, publicarlo en el SIGP y efectuar la debida socialización a las partes interesadas. Importante mantener su actualización y velar por la ejecución periódica de las pruebas respectivas.

1.4.3. Hito 3: Plan de gestión del cambio documentado e implementado.

Sobre este aspecto, se pudo inicialmente evidenciar en el SIPG, en el proceso de Gestión de las Tecnologías de la Información los “Lineamientos para la Gestión de Cambios de Tecnologías de la Información “, versión 2 de enero 2025. En los cuales se 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.

Al respecto, también se evidencia la “Ficha de Gestión del Cambio Uso y Apropiación”, 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:

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

#	Actividad	Objetivo / Descripción	Acciones claves	Stakeholder/ Público
1	Diseñar el Plan de Gestión del Cambio.	Diseñar el Plan de Gestión del cambio identificando pasos y actividades.	N/A	Gestor del cambio
2	Diseño del Plan de Comunicaciones	Diseñar el Plan de Comunicaciones con la información por publicar.	1. Articulación con comunicaciones 2. Definir la estrategia de comunicaciones (canales efectivos, tipos de mensajes, público, actividades)	Gestor del cambio/OAC
3	Diseñar la Capacitación (workshop sensibilización)	Capacitación con puntos claves para el desarrollo de capacidades requeridas.	1. Identificar puntos claves del cambio (la necesidad, argumentos del cambio: beneficios, oportunidades, amenazas) 2. Escribir y estructurar contenidos 3. Generar material con diseño (ppts, infografía)	Gestor del cambio.
4	Realizar matriz de Stakeholders	Grupos de interés gestionados según corresponda	1. Caracterizar roles y responsabilidades en la implementación del sistema de información 2. Identificar los grupos de interés	Gestor del cambio.
5	Alinear Gestión Humana y Comunicaciones como aliados estratégicos.	Movilizar a las áreas de Gestión Humana (GH) y la Oficina Asesora de Comunicaciones (OAC) como aliados estratégicos en el proceso de cambio para la implementación del Sistema de Información.	1. Reunión con GH, OAC y Equipo del proyecto	GH, OAC y Equipo del proyecto
6	Planear Workshops de alineación y sensibilización y Kickoff.	Colaboradores compran el cambio: que se encuentren sensibilizados e informados sobre la necesidad de cambio para adoptar la transformación digital, y se alineen con el propósito del cambio.	1. Planear workshops de alineación y movilización para sensibilizar a los grupos de interés identificados sobre el cambio (fecha, hora, lugar, invitación) 2. Planear KickOff con la población general (fecha, hora, lugar, invitación)	Gestor del cambio
7	Preparar al patrocinador del cambio	Preparar al patrocinador del cambio quien será el promotor visible en la implementación del sistema de información.	1. Apoyar al patrocinador del cambio con los puntos claves del proyecto y la visión	Gestor del Cambio.
8	Realizar workshop sensibilización.	Movilizar a la alta dirección, líderes funcionales y actores identificados como actores estratégicos en el proceso de cambio.	1. Ejecutar el workshop de alineación y sensibilización con los líderes y actores estratégicos 2. Promover el liderazgo, compromiso y construcción del cambio en equipo	Equipo del proyecto.
9	Iniciar plan de comunicaciones	Generar expectativa en el marco del Plan de Comunicaciones para el cambio.	1. Lanzar campaña de expectativa al público general en el marco del Plan de Comunicaciones para el cambio.	OAC.
10	Crear la visión de cambio	Visión del cambio esperado con la implementación del Sistema de Información clara y concreta	1. Concretar la visión del cambio esperado con la implementación del Sistema de Información.	Equipo del proyecto.
11	Definir el propósito e identidad.	Propósito y la identidad del cambio definido en una afirmación de menos de 2 minutos	1. Establecer una declaración con el propósito y la identidad del cambio para transmitirlo en las publicaciones y en el proceso de apropiación del sistema de información, alineado con la cultura. 2. Incluir la visión en el plan de comunicaciones	Equipo del proyecto.
12	Desarrollar expectativa en el Plan de Comunicaciones.	Plan de Comunicaciones para genera expectativa, sensibilización e informa.	1. Ejecutar las actividades y divulgación de información descritas en el Plan de Comunicaciones para generar expectativa y sensibilización.	OAC.
13	Realizar Kick-Off General.	Evento de Kick-Off del proyecto con la población general logra sensibilizar, informar e involucrar en el proceso de cambio que van a enfrentar.	1. Realizar el evento de Kick-Off del proyecto (implementación del Sistema de información) con la población general para sensibilizar, informar e involucrar en el proceso de cambio que van a enfrentar.	Población General.
14	Gestionar Stakeholders	Realizar intervención con los stakeholders identificados de acuerdo con sus roles, responsabilidades y necesidades	Por definir	Equipo del proyecto.
15	Ejecutar los workshop con los Stakeholders (a necesidad)	Desarrollar los workshops (talleres o mesas de trabajo) con los distintos actores identificados entre los grupos de interés, para facilitar el cambio, de acuerdo con sus necesidades	Por definir	Equipo del proyecto.

Fuente: Ficha de Gestión del Cambio Uso y Apropiación – SGI 2025

Recomendación

Importante efectuar la revisión de la ficha, por cuanto fue implementada a mediados de la vigencia 2024.

Asegurarse además que esta herramienta sea debidamente aplicada por las dependencias responsables para proyectos que ameritan la gestión de cambios de TI, con el fin de garantizar que las modificaciones en los servicios y la Infraestructura de la OTIC en Función Pública se realizan de manera controlada y minimizando el riesgo de impacto sobre el negocio.

1.5. Actividad 5: Documentar los planes y las acciones requeridas para restablecer las operaciones misionales de la Función Pública.

Responsables: OTIC, Direcciones Técnicas.

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)

1.5.1. Hito 1: Ficha técnica de ejercicios de Continuidad adelantados/ Hito 3: Resultados de las pruebas.

Sistemas misionales

- **FURAG**

En el DRP del sistema FURAG publicado en el SIGP (versión 5 junio 2025), se evidencia la determinación de las actividades técnicas para las fases de preparación y ejecución de la prueba (Numeral "**9.6.5 Pruebas de recuperación de bases de datos**").

En la vigencia 2024, se adelantaron pruebas de restauración de backup de datos del 02 de septiembre de 2024 en ambiente preproductivo de FURAG, las cuales fueron exitosas, evidenciándose el debido registro en Proactivanet (REQ 2024-062814).

De otro lado, hay un documento que está en construcción denominado "2024-09-09_Plan_recuperacion_servicio_furagiii_nube_publica_v3", el cual posee parte de la información de una ficha técnica para pruebas.

Los soportes mencionados fueron evidenciados en la ruta: \\yaksa.dafp.local\10031GSI\2024\DOCUMENTOS_APOYO\FURAG_III_SIGEP_II_SEM_2_C062\4_EJECUCION\1_TECNICA_FURAG\1_BACKUPS\PRUEBAS_RESTAURACION_BACKUPS.

No obstante, no se videncia una ficha técnica de los ejercicios de continuidad adelantados en la vigencia 2024.

- **SIGEP**

En el DRP del sistema SIGEP publicado en el SIGP (versión 2 diciembre 2024), se evidencia la determinación de las actividades técnicas para las fases de preparación y ejecución de la prueba (Numeral "**Anexo 1. Plan de Pruebas**").

En la presente vigencia se adelantó involuntariamente pruebas de recuperación, debido a que por temas de migración del sistema SIGEP de la nube privada a la infraestructura local On Premise (Servidores, software y bases de datos), hubo la necesidad de aplicar 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)

restauración del sistema con resultados satisfactorios. Al respecto, la OTIC está adelantando actualmente la construcción de un documento denominado “Documentación ejecución planes de recuperación sistemas misionales “, el cual tendrá por objeto compilar los resultados de las pruebas periódicas efectuadas a los DRP de cada sistema.

- **SUIT**

En el DRP del sistema SUIT publicado en el SIGP (versión 3 mayo 2025), se evidencia la determinación de las actividades técnicas para las fases de preparación y ejecución de la prueba (“**4. Fase 3 y 4. Verificar y mejora continua**”).

En la presente vigencia se adelantó involuntariamente pruebas de recuperación, debido a que por temas de migración del sistema SUIT de la nube privada a la infraestructura local On Premise (Servidores, software y bases de datos), hubo la necesidad de aplicar la restauración del sistema con resultados satisfactorios. Al respecto, la OTIC está adelantando actualmente la construcción de un documento denominado “Documentación ejecución planes de recuperación sistemas misionales “, el cual tendrá por objeto compilar los resultados de las pruebas periódicas efectuadas a los DRP de cada sistema.

Sistemas de Apoyo

- **KACTUS**

En el DRP del servicio de la herramienta KACTUS publicado en el SIGP (versión 2 diciembre 2024), no se evidencia la determinación de las actividades técnicas para las fases de preparación y ejecución de la prueba, que harían parte de la ficha técnica.

De otro lado, no se adelantaron pruebas del DRP para la presente vigencia.

- **ORFEO**

Se evidencia la documentación del procedimiento denominado “Plan de recuperación del servicio Orfeo” (Ruta:\\yaksa.dafp.local\10033GPETI\2024\DOCUMENTOS_APOYO \ABEJARANO\ORFEO\HALLAZGO_576), versión de diciembre de 2024, el cual tiene por objeto “Recuperar el servicio de Orfeo por daño físico, daño en la aplicación o inconvenientes en la infraestructura tecnológica.”, en él se pueden apreciar entre otros, las actividades a desarrollar (Descripción, responsables, recursos y tiempo).

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)

Este plan de recuperación a pesar que se encuentra actualizado, no se encuentra con el estándar de presentación y forma como se encuentran los DRP de los sistemas misionales, tampoco ha sido publicado en el SIPG en el proceso de Gestión de las tecnologías de la información.

De otro lado, no se adelantaron pruebas del DRP para la presente vigencia.

1.5.2. Hito 2: Cronograma para el ejercicio de restablecimiento operativo.

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.

.

Recomendaciones

1. El CISO o responsable asignado para efectuar el seguimiento al PECN, debe conocer y mantener el acervo de soportes de las pruebas a todos los DRPs efectuadas durante cada vigencia (Cronogramas de prueba y fichas técnicas y/o informe de resultados de la ejecución).

2. 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.

3. Como se ha venido recomendando en seguimientos de vigencias anteriores, la OTIC en Coordinación con la Dirección Técnica o Dependencia correspondiente, siempre y cuando los recursos financieros y de infraestructura así lo permitan, deben programar mínimo una prueba de cada DRP de los sistemas misionales 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).

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

4. 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.
     - 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.

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)

- 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.

5. 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.

1.6. Actividad 6: Planificar y llevar a cabo el assessment del SGSI.

Responsables: OTIC.

1.6.1. Hito 1: Assessment del SGSI realizados y documentados.

Inicialmente, se aclara que un assessment del Sistema de Gestión de Seguridad de la Información - SGSI es una evaluación que ayuda a las organizaciones a entender su postura actual de seguridad de la información e identifica las áreas que necesitan mejoras, mediante la realización de una evaluación de riesgos.

Esta acción fue desarrollada en el mes de mayo de esta vigencia bajo el apoyo de un aliado estratégico como lo es FORTINET, líder global en soluciones y servicio de ciberseguridad y quien presta algunos servicios contratados por la Entidad. Esta Empresa generó un documento cuyo objetivo fundamental fue brindar al Departamento las recomendaciones y buenas prácticas que permitan un uso óptimo de la tecnología, acompañando el crecimiento organizacional durante el proceso de transformación digital, basado en las recomendaciones del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) a través de su marco de Ciberseguridad que ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y 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)

En este trabajo se Identificaron las condiciones, controles y proyectos necesarios para minimizar los impactos al negocio, generados por ataques de la ciberdelincuencia a la infraestructura de TI, a través del análisis de madurez de procesos, riesgos y arquitectura.

El documento mencionado se denominó "2025-05-05_Cybersecurity_assessment_dafp.ppt" y se evidencia en la ruta: \\yaksa.dafp.local\10030OTIC\2025\DOCUMENTOS_APOYO\SEGURIDAD\PLANES_POLITICAS.

1.7. Actividad 7: Emprender revisiones por la dirección del SGSI regularmente.

Responsables: OTIC, OAP.

1.7.1. Hito 1: Informe del seguimiento realizado por la dirección al SGSI.

Este Hito aún no ha sido efectuado. Tiene fecha de cumplimiento al 30 de diciembre de 2025.

Recomendación

Como se recomendó en el seguimiento efectuado por la Oficina de Control Interno en la vigencia 2024, y acorde a las mejores prácticas derivadas de la norma ISO 27001, se debe realizar y presentar ante el Comité Institucional de Gestión y Desempeño el informe de revisión por la Dirección, el cual permite presentar el estado actual de SGSI, garantizando que sus objetivos continúen siendo adecuados y efectivos y evaluando la validez de los problemas identificados y los riesgos de la Entidad.

1.8. Actividad 8: Aplicar la Mejora Continua al Sistema de Gestión de Seguridad de la Información.

Los planes de mejora se encuentran en tratamiento acorde con el procedimiento interno vigente y controlado a través del SGI.

Para el caso de planes de mejoramiento relacionados con continuidad del negocio, se tienen a la fecha los siguientes hallazgos:

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)

Hallazgo	Fecha registro	Estado	Orientación
570	4 /06/ 2024	ABIERTO	Recopilación hallazgos 261, 267, 269, 295, 296 y 563, relacionados con actualización del BIA y ejecución de pruebas a los DRP de sistemas misionales.
594	22 /11/2024	ABIERTO	Aspectos susceptibles de mejora plan de continuidad de negocio a nivel operativo sistema SIGEP.

Al respecto, no se evidencia que el responsable de seguimiento del PECN efectúe como segunda línea de defensa, seguimiento a la gestión de hallazgos en el plan de mejoramiento institucional y en especial a los que tienen que ver con continuidad de negocio; como se puede observar son hallazgos registrados en la vigencia 2024 y a la fecha no han sido cerrados.

Recomendación

El encargado de la OAP (CISO o responsable respectivo), debe efectuar como segunda línea de defensa el seguimiento continuo a la debida y oportuna gestión de los planes de mejoramiento oficializados en el SGI que impacten la continuidad de negocio, sean estos derivados de auditorías de gestión o por otros escenarios de origen.

De otro lado, a pesar que la continuidad de negocio está inmersa en el SGSI, para el PECN se debería ajustar la orientación de este Hito y el que lo precede, orientándolos al modelo de continuidad de negocio y no al de seguridad de la información.

Conclusiones y Recomendaciones generales

1. Con el fin de mantener la trazabilidad y control de la gestión del PECN, se deben incorporar las actividades determinadas en dicho plan en el módulo de planeación institucional del SGI.

2. 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.

3. 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

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)

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.

4. En lo posible, y hasta donde el presupuesto y la infraestructura técnica lo permita, se deben adelantar ejercicios periódicos de prueba sobre la efectividad de todos los DRPs oficialmente establecidos, tanto a nivel de base de datos como de aplicativo. Tener en cuenta la implementación y uso de las fichas técnicas de prueba recomendadas al interior de este informe.

5. 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: 2025.10.30 14:59:23 -05'00'

Jorge Iván De Castro Barón
Jefe Oficina de Control Interno

INFORME DE SEGUIMIENTO AL PLAN ESTRATÉGICO DE CONTINUIDAD DEL NEGOCIO

Versión 01
Evaluación Independiente
Octubre de 2025

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)