1 OBJETIVO

Definir las actividades relacionadas a Tecnología de Información y Comunicaciones TIC de la Entidad, que se deben ejecutar en una Contingencia Tecnológica a través de un enfoque organizado y consolidado de las etapas de Activación, Recuperación, Restauración y Retorno que hacen parte del Plan de Recuperación de Desastres de la Entidad, con el fin de dar respuesta oportuna en la materialización de un escenario de desastre.

2 ALCANCE

Se inicia con la presentación del informe del incidente al [Comité de DRP] para determinar la posible ejecución del Plan de Recuperación de Desastres de TI; continua, con la ejecución de las actividades de activación, recuperación y restauración; finalizando con las actividades de retorno al estado normal de operación.

3 LÍDER DEL PROCEDIMIENTO

Director de Gestión de Tecnología de Información y Comunicaciones.

4 POLÍTICAS DE OPERACIÓN

- Las políticas de operación del presente procedimiento se encuentran alineadas con las directrices de la Política Continuidad del Negocio que se encuentran dentro del marco de las Políticas Específicas de Seguridad y Privacidad de la Información que la Entidad ha definido.
- El presente procedimiento al igual que el Plan de Recuperación de Desastres que se tenga definido será validado por la ADRES en cabeza de la Dirección de Gestión de Tecnología de Información y Comunicaciones anualmente conforme a lo que se defina dentro del Plan de Seguridad y Privacidad de la Información de cada vigencia.
- Dentro del contexto de este procedimiento, el **Comité DRP** estará compuesto por:
    - Director(a) de la Dirección de Gestión de Tecnologías de Información y Comunicaciones
    - Coordinador Soporte de Tecnologías de Información.
    - Coordinador Administración Base de Datos Única de Afiliados.
    - Coordinador Proyectos de Información
    - Gestor de Operaciones que cumpla las funciones de líder de Seguridad de la Información.
- El presente procedimiento está alineado con los siguientes objetivos de controles ISO 27000:
    - ✓ A17.1.1 Planificación de la continuidad de la seguridad de la información. La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
    - ✓ A17.1.2 Implantación de la continuidad de la seguridad de la información. La organización debería establecer, documentar, implementar y mantener

procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- ✓ A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad. La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
- ✓ A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
- ✓ A.18.1 Cumplimiento de requisitos legales y contractuales. Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

5 REQUISITOS LEGALES Ver normograma del proceso

6 DEFINICIONES Ver Glosario general

7 DESARROLLO DEL PROCEDIMIENTO

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Presentar informe del incidente al [Comité de DRP]	El Gestor de Operaciones – Coordinador del Grupo de Gestión de Soporte a la Tecnologías o el Gestor de Operaciones responsable del caso que ha sido catalogado como incidente determina el impacto de este y valida la aplicación de las estrategias de recuperación que se encuentran definidas en el documento "Plan de Recuperación de Desastres – DRP" y estima el tiempo de la solución del incidente. Con dicho contexto informa al [Comité de DRP] para la determinación de la activación o no del Plan de Recuperación de Desastres.	Gestor de Operaciones	Módulo de Mesa de Servicio
2 **PC**	Validar informe para activación del Plan de Recuperación de Desastres	El [Comité de DRP] una vez conozca la información reportada en la actividad anterior, con el propósito de determinar la pertinencia o no de activación del escenario de Recuperación de Desastres, realiza la validación del informe presentado. ¿Se requiere activación del Plan de Recuperación de Desastres? **SI:** Comunica a los líderes técnicos y al Comité Institucional de Gestión y	[Comité de DRP]	Decisión registrada en el Módulo mesa de Servicio

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Desempeño, con el fin de adelantar los preparativos para la ejecución de los procedimientos de recuperación de los Servicios y Sistemas de Información. Continuando así con la actividad No. 3. **NO:** Retroalimenta a quien reportó la ocurrencia del Incidente indicando el porqué de la no pertinencia de activación del Plan, lo cual quedará registrado en el Módulo mesa de Servicio para continuar atendiendo conforme al procedimiento de Gestión de Incidentes y se cierra el presente procedimiento Toda evidencia, deberá quedar registrada dentro del módulo mesa de Servicio por parte de la persona que reportó la ocurrencia del Incidente.		
3	Determinar orden de activación de Servicios y Sistemas de Información	El [Comité de DRP], una vez se determina la activación del escenario de Recuperación de Desastres definen el orden de activación de los Servicios y Sistemas Información con base a los procesos críticos y el calendario de ejecución de estos, para esto tendrá en cuenta lo definido en: ✓ Plan de Continuidad del Negocio ✓ *Plan de Recuperación de Desastres – DRP* ✓ Guías de recuperación de los Servicios y Sistemas de Información. Como evidencia del orden de activación se tendrán las observaciones consignadas en el listado de asistencia de la reunión o en su defecto en el formato de acta vigente dentro de la entidad.	[Comité de DRP]	Lista de asistencia Formato de acta
4	Declarar la contingencia al del Comité Institucional de Gestión y Desempeño	El director de Gestión de Tecnología de Información y Comunicaciones contactará a los integrantes del **Comité Institucional de Gestión y Desempeño** para analizar, evaluar y tomar decisiones basados en la información que se tenga acerca del incidente reportado e iniciar las actividades asociadas a sus roles de	Director de Gestión de Tecnología de Información y Comunicaciones	Acta del Comité

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Contingencia conforme con lo definido dentro del **Plan de Continuidad del Negocio** de la Entidad.		
5	Activar Servicios transversales	Los Integrantes del Grupo Interno de Soporte a las Tecnologías, una vez sea definido el orden de activación de los Servicios y Sistemas de información, activan los servicios transversales, conforme a las guías de recuperación de estos y de los Sistemas de Información afectados. Paso seguido de la activación, informarán vía correo electrónico a los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información.	Integrantes del Grupo Interno de Soporte a las tecnologías	Correo electrónico
6	Activar Sistemas de Información	Los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información, una vez sean notificados de la activación de los servicios transversales y con el propósito de dar acceso a los usuarios funcionales activan los Servicios o Sistemas de Información a su cargo, seguirán los pasos definidos en las Guías de recuperación de los Servicios y Sistemas de información que fueron afectados.	Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información	En cada sistema de información
7 **PC**	Validar funcionalidad de los Servicios y Sistemas de Información	Los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información, una vez realicen la activación de los Servicios y Sistemas de Información, con el propósito de habilitar el acceso a los usuarios, validan si se encuentran debidamente habilitados los Servicios y Sistemas de información a los cuales ingresaran estos. ¿Está debidamente habilitado el acceso? **SI:** Se continua con la actividad No. 8. **NO**: Se retorna a la actividad No. 6 hasta que los Servicios y Sistemas de Información se encuentren disponibles.	Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información	Pantallazos de validaciones realizadas

No	Actividad	Descripción de la Actividad	Responsable	Registro
		En cualquiera de los dos casos se dejará como evidencia pantallazos de la validación realizada, los cuales se almacenarán en la ubicación de la herramienta colaborativa que se defina en su momento.		
8 **PC**	Validar posible pérdida de información	Los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información, posteriormente a la activación de los Sistemas de Información; con el propósito de evaluar el punto objetivo de recuperación RPO de estos, determinan la posibilidad de pérdida de información desde la fecha de ocurrencia del incidente frente al último proceso de respaldo de información realizado conforme a la política de copias de respaldo de los servidores e información alojados en el centro de datos principal. ¿Hubo perdida de información? **SI**: Se reportará la materialización de un Riesgo de Seguridad de la Información conforme con lo definido en los procedimientos de Gestión de Incidentes de Seguridad y Gestión de Riesgos y se continúa con la actividad No. 9. **NO**: Se continúa con la actividad No. 9.	Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información	Reporte de materialización de riesgos
9	Habilitar ingreso a usuarios a los sistemas de información	Los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información, posterior a la verificación del RPO sobre estos Servicios y Sistemas; con el propósito de permitir el trabajo de los usuarios, habilitan el ingreso y operación dentro de estos. Dicha habilitación se dará conforme con el orden que se ha establecido dentro de la actividad No. 3 "Determinar orden de activación de Servicios y Sistemas de Información".	Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información	Sistemas de Información
10	Monitorear los servicios y sistemas de información	Los Integrantes del Grupo Interno de Gestión de Operaciones de Sistemas de Información, una vez los usuarios se encuentren trabajando dentro de los	Integrantes del Grupo Interno de Gestión de	Herramientas de monitoreo

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Servicios y Sistemas de información que fueron habilitados, con el propósito de conocer el estado de uso y rendimiento de la plataforma, a través de las herramientas de monitoreo que se tengan para tal fin; validaran el comportamiento de la RED, Servicios, Servidores, Aplicaciones y Bases de datos. En caso de presentarse alguna situación anómala se debe definir el plan a seguir para asegurar la operatividad dentro del escenario de contingencia que se ha activado. Cabe aclarar que esta actividad se continuará realizando constantemente conforme a la periodicidad que se defina en el escenario de contingencia y paralelamente se iniciará la siguiente actividad. El fin de esta actividad se dará una vez se haya ejecutado el plan de retorno a operación normal.	Operaciones de Sistemas de Información	
11	Evaluar detalladamente el estado de la plataforma tecnológica afectada	Con el fin de definir el plan de retorno al escenario normal, el [Comité de DRP] realiza la evaluación de los daños producto de la ocurrencia incidente que obligó la activación del Escenario Contingente y establecen los mecanismos necesarios de recuperación de la plataforma tecnológica. Adicionalmente, determinan si se requiere recursos financieros o humanos para llevar acabo la restauración. En ese sentido, el director de Gestión de Tecnología de Información y Comunicaciones realiza la solicitud vía correo electrónico ante la Dirección Administrativa y Financiera.	[Comité de DRP]	Correo electrónico (si requiere)
12	Determinar el plan de restauración de la	El [Comité de DRP], una vez se cuente con la evaluación detallada del estado de la plataforma tecnológica afectada y cuente con los recursos financieros o humanos requeridos, con el propósito	[Comité de DRP]	Plan de restauración de la plataforma tecnológica

No	Actividad	Descripción de la Actividad	Responsable	Registro
	plataforma tecnológica	de definir el retorno a la operación normal, define el plan de restauración de la plataforma tecnológica, el cual es compartido por parte del director de Gestión de Tecnología de Información y Comunicaciones al **Comité Institucional de Gestión y Desempeño.**		
13	Ejecutar plan de retorno a la operación normal	Con el propósito de recuperar la operación en el escenario normal, los integrantes de los grupos Internos de Soporte a las tecnologías y Gestión de Operaciones, ejecutan el plan de retorno a la operación normal. Una vez, se realice el retorno a la operación normal, se informa vía correo electrónico por el coordinador de Soporte de Tecnología o el coordinador de Gestión de Operaciones al director de Gestión de Tecnología de Información y Comunicaciones	Integrantes de los grupos Internos de Soporte a las tecnologías y Gestión de Operaciones de Sistemas de Información	Correo electrónico
14 **PC**	Verificar la integridad de la información	Los Integrantes de los grupos Internos de Soporte a las tecnologías y Gestión de Operaciones, una vez haya finalizado el plan de retorno, validan que la información en las diferentes bases de datos se encuentre integra respecto a la que se encontraba en el escenario de recuperación de desastres. ¿Se presentaron inconsistencias durante el proceso de recuperación? **SI:** Se retorna a la actividad No. 13. Es importante tener en cuenta que, en caso de que al verificar en varias oportunidades que la información ha perdido su integridad, se reportará la materialización de un Riesgo de Seguridad de la Información conforme con lo definido en el procedimiento de Gestión de Incidentes de Seguridad y Gestión de Riesgos, con los cuales se continúa. **NO:** Se continua con la actividad No. 15.	Integrantes de los grupos Internos de Soporte a las tecnologías y Gestión de Operaciones de Sistemas de Información	Reporte de materialización de riesgos

No	Actividad	Descripción de la Actividad	Responsable	Registro
15	Notificar finalización del plan de retorno	El director de Gestión de Tecnología de Información y Comunicaciones, una vez los Integrantes de los grupos Internos de Soporte a las Tecnologías y Gestión de Operaciones hayan finalizado el retorno al escenario normal de operación, con el fin de iniciar actividades en este escenario, notificará al **Comité Institucional de Gestión y Desempeño** indicando que la ejecución del plan de retorno ha finalizado. Dicha notificación la realizará a través de correo electrónico.	Director de Gestión de Tecnología de Información y Comunicaciones	Correo electrónico notificando la finalización del plan de retorno
16	Documentar lecciones aprendidas	El [Comité de DRP] una vez se encuentre estable la operación en su escenario normal, con el propósito de contar con una base de conocimientos, documentarán las acciones realizadas en donde se deben indicar: • Tiempo total del escenario de Recuperación de desastre. • Servicios, Sistemas de Información afectados durante el escenario • Hechos más relevantes encontrados dentro del escenario. • Inconvenientes y acciones de respuesta encontrados dentro del escenario. • Riesgos materializados • Acciones de mejora aplicables al Plan de Recuperación de Desastres y procedimientos asociados. Toda esta documentación quedará asociada en un informe de Recuperación de Desastres que posteriormente el director de Gestión de Tecnología de Información y Comunicaciones podrá presentar al Comité Institucional de Gestión y Desempeño. **FIN DEL PROCEDIMIENTO.**	[Comité de DRP]	Informe de Recuperación de Desastres

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Asesor del proceso
01	15 de agosto de 2020	Emisión y Publicación inicial	Juan Guillermo Corredor - OAPCR
02	18 de marzo de 2020	Actualización procedimiento, políticas de operación.	Olga Marcela Vargas Valenzuela Asesor OAPCR
02	*9 de julio de 2020*	Actualización código por cambio de nombre del proceso de GSTE a OSTI. No se genera nueva versión debido a que no se modifica contenido del procedimiento y por lo tanto no requiere aprobación por parte del líder del proceso.	Olga Vargas Asesor OAPCR
03	*30 de diciembre de 2021*	Actualización del flujo de las actividades	Olga Marcela Vargas Valenzuela - Asesor OAPCR Eliana Rodriguez Gomez – Gestor de Operaciones OAPCR

9. ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Juan Carlos Escobar Baquero Gestor de Operaciones - Dirección de Gestión de Tecnologías de Información y Comunicaciones **Guillermo Manuel Benitez Rodriguez** Gestor de Operaciones – Coordinador de Grupo interno de Proyectos de Información	**Carlos Andrés Ruiz Romero** Gestor de Operaciones – Grupo Gestión Soporte a las Tecnologías	**Juan Carlos Mendoza Pedraza** Director de Gestión de Tecnologías de Información y Comunicaciones