CONTENIDO

1 OBJETIVO 3
2 DESTINATARIOS 3
3 GLOSARIO 3
4 REFERENCIAS NORMATIVAS 4
5 GENERALIDADES 5
5.1 POLÍTICAS DEL PROCEDIMIENTO 6
5.2 INTEGRACIÓN CON OTRAS PRACTICAS DE GESTIÓN ITIL 7
6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO 8
7 DESCRIPCIÓN DE ETAPAS Y ACTIVIDADES 10
7.1 Definir planes, alcance y políticas para la Gestión de la Continuidad del servicio de ti 10
7.1.1 Realizar y mantener actualizadas las políticas de Continuidad de Servicios de TI. 10
7.1.2 Definir alcance y responsabilidades. 10
7.1.3 Asignar el personal especializado en recuperación de los servicios de TI. 10
7.2 dEFINIr Requisitos y Estrategias 11
7.2.1 Realizar Análisis de Impacto (BIA). 11
7.2.2 Realizar Análisis de Riesgo y establecer medidas de tratamiento del riesgo. 11
7.2.3 Establecer la estrategia para la Continuidad del Servicio de TI 11
7.2.4 Presentar el plan para validación y aprobación 11
7.2.5 Publicar el Plan de Recuperación ante Desastres. 12
7.3 Implementar el Plan de recuperación ante desastres 12

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Yeison Latorre Ruiz Cargo: Coordinador Grupo de Trabajo de Servicios Tecnológicos	Nombre: Francisco Andrés Rodríguez Eraso Cargo: Jefe Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2020-12-03

7.3.1 Adquirir recursos e infraestructura necesaria 12
7.3.2 Ejecutar la solución del Plan de Recuperación ante Desastres..... 12
7.4 REALIZAR ACTIVIDADES DE OPERACIÓN REGULAR DEL SERVICIO 12
7.4.1 Socializar y sensibilizar a los servidores públicos o contratistas. 12
7.4.2 Revisar periódicamente el Plan de Recuperación ante Desastres. ... 13
7.4.3 Realizar Pruebas al DRP. 13
7.4.4 Generar informes. 13
7.4.5 Realizar ajustes al Plan 13
7.4.6 Ejecutar el Plan de Recuperación ante Desastres y retornar el servicio a su operación normal 14
7.4.7 Continuar la operación del servicio de acuerdo con el Plan de Recuperación ante Desastres. 14
8 DOCUMENTOS RELACIONADOS. 14
9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 14

1 OBJETIVO

Establecer los criterios de entrada y definiciones necesarias para la realización del Plan de Recuperación ante Desastres – DRP, que garantice la continuidad del servicio de TI, el cual se encuentra enmarcado dentro del Plan de Continuidad de Negocio, a través del desarrollo de políticas, actividades, condiciones que garanticen el cumplimiento normativo, alcance, asignación de recursos y tiempos requeridos para su realización.

2 DESTINATARIOS

Este documento aplica a todos aquellos funcionarios o contratistas de la Superintendencia de Industria y Comercio, en adelante SIC, que participen directa o indirectamente en la Gestión de la Continuidad de los Servicios de TI y de recuperación ante desastres – DRP, para la infraestructura de TI considerada como crítica para los procesos misionales de la SIC.

3 GLOSARIO

AMENAZA: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización[1].

BCP - BUSINESS CONTINUITY PLANNING: planeación de Continuidad del Negocio. Metodología que permite la preparación del negocio ante futuros incidentes que le puedan poner en peligro o riesgo.

BIA - BUSINESS IMPACT ANALYSIS: análisis de Impacto del Negocio. Es la actividad de la Gestión de Continuidad del negocio que identifica las funciones vitales del negocio. El BIA define los requerimientos en términos de recuperación para los servicios de TI.

DRP - DISASTER RECOVERY PLAN: Plan de Recuperación ante Desastres. Este documento orienta a la entidad para responder ante una interrupción (desastre o afectación de los servicios de TI) y ayuda a reanudar, recuperar y restaurar los servicios de TI de acuerdo con sus objetivos de continuidad de negocio. Involucra procesos, tecnología y recurso humano para la continuidad del servicio de TI.

IMPACTO: son las consecuencias que puede ocasionar a la organización la materialización del riesgo.

[1] Guía para la administración del riesgo y diseño de controles. Departamento Administrativo de la Función Publica

ITIL: conjunto de mejores prácticas destinadas a mejorar la gestión y provisión de servicios TI.

OTI: Oficina de Tecnología e Informática.

RIESGO: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE TI: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos sobre proceso de TI.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: probabilidad de que suceda algún evento que afecta la confidencialidad, disponibilidad e integridad de la información.

USUARIO: funcionario o Contratista de la SIC que solicita un acceso para utilizar un servicio o un grupo de servicios proporcionados por la Oficina de Tecnología e Informática- OTI.

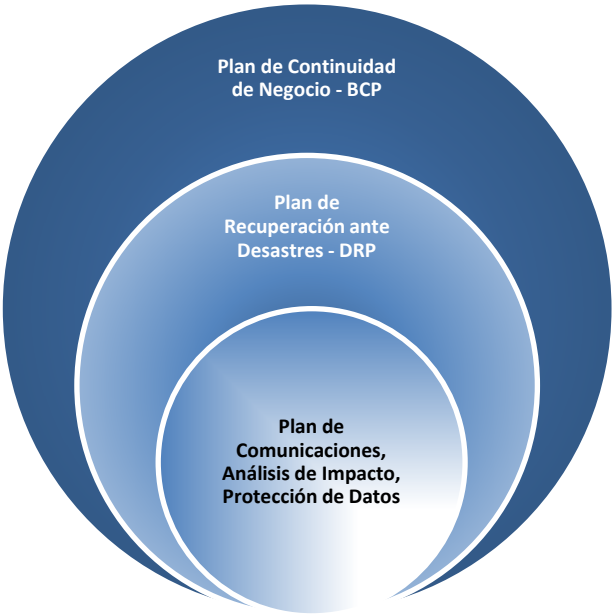
VULNERABILIDAD: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos de información.

4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Decreto Nacional	1008 del 14 de junio de 2018	Política de Gobierno Digital	Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2	Aplicación total
Norma Técnica Colombiana	27001 / 2013	Tecnología de Información, Técnicas de seguridad Sistemas de gestión de la seguridad de la información	Ítem A.17	Aspectos de seguridad de la información, de la Gestión de Continuidad de Negocio.

5 GENERALIDADES

En la actualidad todas las organizaciones sin importar su tamaño deben evaluar y tomar las acciones para garantizar que su información se mantenga a salvo de factores que pueden causar daños o perdidas debido a situaciones como; terremotos, tsunamis, incendios, actividades volcánicas, inundaciones, ataques cibernéticos, guerras, entre otros, por lo mencionado anteriormente se debe tomar en cuenta que el Plan de Continuidad de Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), aun cuando son de vital importancia para la Contingencia no son lo mismo, como se ve en la siguiente imagen:



Estas situaciones, que afectan los procesos críticos los cuales están ligados al área/proceso tecnológico, en caso de que un proceso clave se detenga prolongadamente, la Entidad puede sufrir consecuencias negativas desde pérdidas financieras, problemas de reputación o hasta el cierre de la misma (en caso de un desastre de grandes magnitudes). Por lo tanto, es importante contar con un Plan de Recuperación ante Desastres (DRP) y un Plan de Continuidad de Negocio (BCP), pensado y desarrollado por la entidad, garantizando la prestación del servicio.

La Superintendencia de Industria y Comercio en procura de garantizar la prestación de los servicios, está desarrollando la implementación de un Plan de Recuperación ante Desastres (DRP), para proteger los recursos tecnológicos que soportan sus procesos misionales y de apoyo de forma permanente, ante la ocurrencia de

eventos adversos, velando especialmente por la seguridad de sus funcionarios proveedores y contratistas.

Para los efectos del desarrollo del Plan de Recuperación ante Desastres (DRP), se tomará como referencia la norma ISO 22301, con el fin de asegurar y contar con un marco normativo que permita acceder a las mejores prácticas ya definidas en dicha norma, utilizadas a nivel mundial.

De igual forma, el Plan de Recuperación ante Desastres (DRP) y demás documentos relacionados deben ser revisados anualmente para asegurar su vigencia, cuando se presenten cambios significativos en la Superintendencia y/o cambios en la normatividad vigente.

Nota 1: Los roles y responsabilidades se encuentran detallados en el Anexo 1 “Roles y Responsabilidades – Gestión de Continuidad del Servicio de TI”.

5.1 POLÍTICAS DEL PROCEDIMIENTO

5.1.1 El Plan de Recuperación ante Desastres (DRP) definido por la entidad, debe ser revisado anualmente, o cuando se realice un cambio importante en la infraestructura de TI, o ante requerimientos normativos.

5.1.2 Las pruebas del DRP deben ser realizadas anualmente, o cuando se realice un cambio importante en la infraestructura de TI o cuando se realicen cambios en la normatividad vigente, dichas pruebas pueden ser totales o parciales.

5.1.3 Todo Plan de Recuperación ante Desastres debe contar con su análisis de impacto al negocio (BIA), Análisis de Riesgos y sus líneas de tiempo.

5.1.4 Debe existir una copia física y/o una digital de las últimas versiones del Plan de Recuperación ante Desastres fuera de las instalaciones donde se presta el servicio.

5.1.5 El personal especializado en recuperación de los servicios de TI, es el que ejecuta de manera adecuada las actividades necesarias para el desarrollo normal del plan.

5.1.6 El Plan de Recuperación ante Desastres debe ser divulgado como una parte importante de Sistema de Gestión de Seguridad de la Información.

5.1.7 La programación de las pruebas del DRP debe indicar cómo, cuándo y por quién se van a realizar las actividades requeridas para verificar cada uno de los elementos del plan.

5.2 INTEGRACIÓN CON OTRAS PRACTICAS DE GESTIÓN ITIL

- Mesa de Servicios: punto único de contacto con los usuarios para los servicios de TI contratados.

- Gestión de Cambios: debe tener en cuenta el impacto de todos los cambios en los planes de continuidad. Si los cambios que se van a implementar impactan algún plan de continuidad, debe asegurarse de que se actualiza el plan como parte del cambio. El propio plan debe estar bajo el control de Gestión del Cambio.

- Gestión de Incidentes y problemas: los incidentes pueden revestir la forma de grandes incidentes y desastres. Se debe acordar y documentar criterios claros para la invocación de los planes de ITSCM.

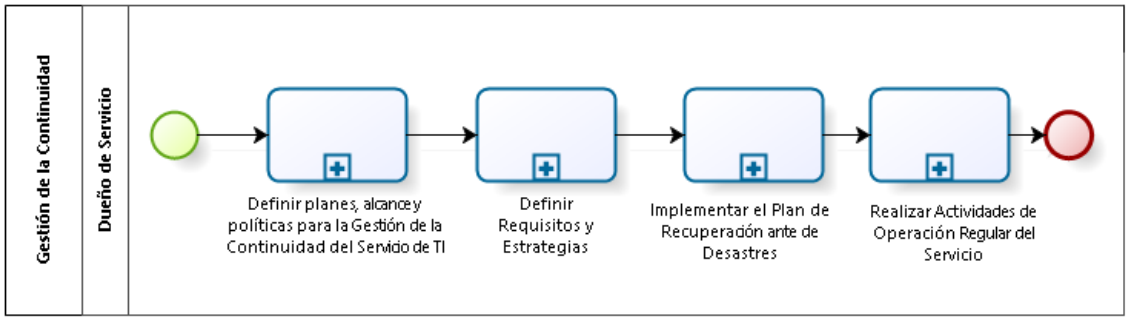
- Gestión de la Disponibilidad: se debe realizar un análisis de riesgos e implementar respuestas a los riesgos, en estrecha coordinación con el procedimiento de disponibilidad para optimizar la mitigación de riesgos.

- Gestión de la Capacidad: en este procedimiento, se debe asegurar los recursos suficientes para permitir la recuperación de los equipos de reemplazo después de un desastre.

- Gestión de la Configuración: en este procedimiento se documenta los componentes de la infraestructura y la relación entre esos componentes. Esta información es necesaria en todas las etapas del ciclo de vida ITSCM y manteniendo al mismo tiempo los planes y las instalaciones de recuperación.

- Gestión de la Seguridad: al realizar los análisis de riesgo, es muy importante para garantizar que se aplican los mismos controles de seguridad de la operación.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO



No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**DEFINIR PLANES, ALCANCE Y POLÍTICAS PARA LA GESTIÓN DE LA CONTINUIDAD DEL SERVICIO DE TI**	SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI Políticas y normatividad vigente. Plan de Recuperación ante desastres. Formato Pruebas de DRP	Esta etapa consiste en definir las políticas para el procedimiento, y presenta las siguientes actividades: - Realizar y mantener actualizadas las políticas de Continuidad de Servicios de TI. - Definir alcance y responsabilidades. - Asignar personal especializado en recuperación de los servicios de TI.	Dueño del Servicio	Políticas y Roles ajustados o definidos Personal especializado en recuperación de los servicios de TI conformado y asignado Plan de Recuperación ante desastres, formulado. Formato Pruebas de DRP
2	**DEFINIR REQUISITOS Y ESTRATEGIAS**	Políticas ajustadas o definidas Plan de Recuperación ante desastres, formulado.	Esta etapa tiene como fin documentar el DPR – para dar continuidad al Servicio de TI y presenta las siguientes actividades: - Realizar Análisis de Impacto (BIA). - Realizar Análisis de Riesgo y establecer medidas de tratamiento del riesgo. - Establecer la estrategia para la	Dueño de Servicio Personal especializado en recuperación de los servicios de TI	Análisis de Impacto al Negocio documentado en el DRP. Riesgos Identificados Plan de Gestión de Riesgos Plan de Recuperación ante

			continuidad del Servicio de TI - Presentar el plan para validación y aprobación. - Publicar el Plan de Recuperación ante Desastres.		desastres / DRP aprobados.
3	**IMPLEMENTAR EL PLAN DE RECUPERACIÓN ANTE DE DESASTRES**	Plan de Recuperación ante desastres / DRP Soluciones ejecutadas (Prerrequisitos)	Esta etapa consiste en realizar las actividades necesarias para ejecutar el Plan de Recuperación ante Desastres y presenta las siguientes actividades: - Adquirir recursos e infraestructura necesaria - Ejecutar la solución del plan de recuperación ante desastres.	Personal especializado en recuperación de los servicios de TI.	Recursos Adquiridos. Soluciones configuradas
4	**REALIZAR ACTIVIDADES DE OPERACIÓN REGULAR DEL SERVICIO**	Plan de Recuperación ante desastres / DRP. Resultados de las Pruebas	En esta etapa se describen las actividades para la revisión y gestión de la continuidad del servicio de TI mediante el DPR y presenta las siguientes actividades: - Socializar y sensibilizar a los servidores públicos o contratistas. - Revisar periódicamente el plan ante desastres. - Realizar Pruebas de DRP. - Generar informes. - Realizar ajustes al Plan. - Ejecutar el Plan de Recuperación ante Desastres y retornar el servicio a su operación normal.	Dueño de Servicio. Personal especializado en recuperación de los servicios de TI.	Reuniones de socialización y sensibilización en el DRP. Actualizaciones Posibles al Plan de Recuperación ante desastres / DRP Resultados de las Pruebas Resultados

			- Continuar la operación del servicio de acuerdo con el Plan de Recuperación ante Desastres.		

7 DESCRIPCIÓN DE ETAPAS Y ACTIVIDADES

7.1 DEFINIR PLANES, ALCANCE Y POLÍTICAS PARA LA GESTIÓN DE LA CONTINUIDAD DEL SERVICIO DE TI

7.1.1 Realizar y mantener actualizadas las políticas de Continuidad de Servicios de TI.

El dueño del servicio debe establecer y/o actualizar variables de entrada y definiciones que estarán cubiertas dentro del DRP requerido por la SIC y definidas por la OTI, tales como políticas, condiciones, alcance, definición de los recursos y tiempos requeridos para realizar los planes.

7.1.2 Definir alcance y responsabilidades.

El líder de la práctica ITIL y el Gestor de Continuidad deben establecer el alcance y las responsabilidades de los servidores públicos o contratistas que se involucrarán en la definición y desarrollo del Plan de Recuperación ante Desastres, lo anterior a fin de tener roles definidos y necesarios para ejecución.

Los roles deben ser aprobados por del Dueño de Servicio.

7.1.3 Asignar el personal especializado en recuperación de los servicios de TI.

Definir un equipo de trabajo para llevar a cabo el DRP, este equipo trabajará en diversas actividades según el plan definido por la SIC.

Esta actividad se encuentra a cargo del Dueño de Servicio con el apoyo del Líder de la Práctica ITIL.

7.2 DEFINIR REQUISITOS Y ESTRATEGIAS

7.2.1 Realizar Análisis de Impacto (BIA).

Realizar un análisis del impacto del negocio para identificar los procesos más críticos de la SIC, teniendo en cuenta la gestión de riesgos, arquitectura de TI y normatividad vigente. Lo anterior como insumo para el DRP.

Identificar el alcance de su gestión y la problemática para solucionar lo identificado.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI.

7.2.2 Realizar Análisis de Riesgo y establecer medidas de tratamiento del riesgo.

Realizar una evaluación de la vulnerabilidad y nivel de amenaza a los servicios de TI. Una vez identificados los riesgos, se debe revisar cada uno de los planes de respuesta para gestionarlos, por ejemplo, Instalación de UPS y energía de reserva para los equipos de la entidad. Lo anterior debe estar ajustado con la metodología de gestión de riesgos de la Entidad, SC01-P03 – Metodología para la Administración de Riesgos.
Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI con el apoyo del Gestor de Continuidad y Gestor de Riesgos.

7.2.3 Establecer la estrategia para la Continuidad del Servicio de TI

Esta actividad se encuentra a cargo del Dueño de Servicio, Personal especializado en recuperación de los servicios de TI y Líder de la Práctica ITIL con el apoyo del Gestor de Continuidad, deben establecer el plan que se llevará a cabo para la recuperación de los servicios de TI en caso de una grave interrupción de estos, debe incluir las actividades y las líneas de tiempo definidas para ejecutar dicho plan e indicar costos asociados.

7.2.4 Presentar el plan para validación y aprobación

Exponer el Plan de Recuperación ante Desastres para validación y aprobación, en las reuniones de gestión en cabeza del jefe de la OTI, quien debe revisar que el plan este adecuadamente documentado, que todas las propuestas sean viables para la recuperación de los servicios. Finalmente, el jefe de la OTI debe aprobar el plan o recomendar los ajustes necesarios para su aprobación.

Estas reuniones de gestión están conformadas por el Jefe de Oficina de la OTI como Dueño del Servicio y otras partes interesadas (áreas misionales y de apoyo), por demanda de la Jefatura de OTI y Líder de la Práctica ITIL.

7.2.5 Publicar el Plan de Recuperación ante Desastres.

Se debe publicar y comunicar el Plan de Recuperación ante Desastres a todos los interesados (áreas misionales, estratégicas y de apoyo, directivos, servidores públicos, contratistas y proveedores) para que conozcan cómo se debe proceder en caso de una grave interrupción.

Esta actividad se encuentra a cargo del Dueño de Servicio y del Líder de la Práctica ITIL.

7.3 IMPLEMENTAR EL PLAN DE RECUPERACIÓN ANTE DESASTRES

7.3.1 Adquirir recursos e infraestructura necesaria

Revisar los recursos y la infraestructura necesaria para llevar a cabo el Plan de Recuperación ante Desastres, y soportar que se encuentren disponibles y en óptimas condiciones para permitir la continuidad de los servicios.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI, Líder de la Práctica ITIL y Dueño del Servicio.

7.3.2 Ejecutar la solución del Plan de Recuperación ante Desastres.

Gestionar las actividades necesarias para la ejecución del Plan. Evaluar si estas actividades requieren una ventana de mantenimiento para ejecutarlas, si se requiere, seguir el proceso de Gestión de Cambios.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI.

7.4 REALIZAR ACTIVIDADES DE OPERACIÓN REGULAR DEL SERVICIO

7.4.1 Socializar y sensibilizar a los servidores públicos o contratistas.

Socializar y sensibilizar los servidores públicos o contratistas involucrados, para que conozcan las actividades que se deben ejecutar al momento de tener que implementar el Plan de Recuperación ante Desastres a un servicio.

Esta actividad se encuentra a cargo del Dueño de Servicio con el apoyo del Líder de la Práctica ITIL.

7.4.2 Revisar periódicamente el Plan de Recuperación ante Desastres.

Al menos una vez al año, cuando exista un cambio normativo, cuando exista un cambio importante en la infraestructura, para mantener actualizado el plan y los documentos relacionados.

Esta actividad se encuentra a cargo del Dueño de Servicio con el apoyo del Líder de la Práctica ITIL y el Gestor de Continuidad.

7.4.3 Realizar Pruebas al DRP.

Se deben realizar pruebas del Plan de Recuperación ante Desastres, totales o parciales, para identificar si las actividades estipuladas son las adecuadas, de acuerdo con lo definido en el alcance de la prueba.

Estas pruebas y su ventana de ejecución deben seguir los lineamientos del procedimiento DE04-P04 de control de Cambios y se deben registrar en el Formato de Pruebas de DRP.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI y del Líder de la Práctica ITIL.

7.4.4 Generar informes.

Realizar un informe cada que se pruebe el Plan de Recuperación ante Desastres, que contenga los resultados obtenidos en las pruebas, recomendaciones, metodología y conclusiones.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI.

7.4.5 Realizar ajustes al Plan

Revisar y realizar los ajustes necesarios al Plan de Recuperación ante Desastres, en caso de encontrar alguna falla o cambios normativos o de infraestructura, para poder llevar a cabo las pruebas totales o parciales.

Esta actividad se encuentra a cargo del Personal especializado en recuperación de los servicios de TI y Dueño de Servicio.

7.4.6 Ejecutar el Plan de Recuperación ante Desastres y retornar el servicio a su operación normal

Ejecutar el plan sólo cuando ocurra una grave interrupción de alguno de los servicios definidos en el Plan de Recuperación ante Desastres.

Si el desastre ya fue solucionado, la operación del servicio deberá retornar a la normalidad incluyendo lo definido en el Plan de Comunicaciones implícito en el Plan de Continuidad del Negocio.

De ser necesario, se revisará y realizarán ajustes necesarios al Plan de Recuperación ante Desastres.

Esta actividad se encuentra a cargo de todos los roles que intervienen en este procedimiento.

7.4.7 Continuar la operación del servicio de acuerdo con el Plan de Recuperación ante Desastres.

Si el desastre no ha sido solucionado, se continuará operando desde el sitio alterno con la infraestructura y el recurso establecido en el Plan de Recuperación ante Desastres, hasta que la situación se haya normalizado.

Esta actividad se encuentra a cargo de todos los roles que intervienen en este procedimiento.

8 DOCUMENTOS RELACIONADOS

- DE04-P04 Procedimiento de control de cambios
- Plan de Recuperación ante Desastres – Documento Confidencial que no será publicado en el Sistema Integral de Gestión Institucional - SIGI
- Formato Artefacto Detalle Pruebas DRP.
- Metodología BIA.
- Anexo 1 “Roles y Responsabilidades – Gestión de Continuidad del Servicio de TI”.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Creación del documento.

_____

Fin documento