Contenido

[1. INTRODUCCIÓN 3](#_Toc99640124)

[2. OBJETIVOS 3](#_Toc99640125)

[2.1. OBJETIVO GENERAL 3](#_Toc99640126)

[2.2. OBJETIVOS ESPECÍFICOS 3](#_Toc99640127)

[3. TERMINOS Y DEFINICIONES 4](#_Toc99640128)

[4. ALCANCE 6](#_Toc99640129)

[5. ANALISIS Y JUSTIFICACIÓN DEL PLAN 6](#_Toc99640130)

[6. ESTRATEGIA GENERAL DE RECUPERACIÓN 8](#_Toc99640131)

[6.1. ANÁLISIS Y EVALUACIÓN DE DAÑOS 9](#_Toc99640132)

[6.2. ACTIVACIÓN DEL DRP 10](#_Toc99640133)

[6.3. MECANISMOS DE COMUNICACIÓN 11](#_Toc99640134)

[7. EQUIPO DE RECUPERACIÓN 11](#_Toc99640135)

[7.1. ESTRUCTURA 11](#_Toc99640136)

[7.1.1. LÍDER DRP (LÍDER DE RECUPERACIÓN TECNOLÓGICA) 12](#_Toc99640137)

[7.1.2. EQUIPO EVALUADOR DE DAÑOS 13](#_Toc99640138)

[7.1.3. EQUIPO COORDINADOR DE DRP 14](#_Toc99640139)

[7.1.4. COORDINADOR DE CENTRO DE DATOS ALTERNO 15](#_Toc99640140)

[7.1.5. EQUIPO DE RECUPERACIÓN DE DRP 16](#_Toc99640141)

[7.2. LINEA DE SUCESIÓN 18](#_Toc99640142)

[7.3. ÁRBOL DE LLAMADAS 18](#_Toc99640143)

[8. PROCEDIMIENTO DE ACTIVACIÓN Y RETORNO DE SERVICIOS 22](#_Toc99640144)

[9. PLAN DE PRUEBAS DEL SITIO ALTERNO 24](#_Toc99640145)

[A. TIPO DE PRUEBAS 24](#_Toc99640146)

[B. FRECUENCIA DE LAS PRUEBAS 25](#_Toc99640147)

[C. RESULTADOS Y EVALUACION DE LAS PRUEBAS 25](#_Toc99640148)

[D. COORDINACIÓN CON LAS ÁREAS USUARIAS 26](#_Toc99640149)

[10. DISTRIBUCIÓN, DISPONIBILIDAD Y MANTENIMIENTO DEL PLAN 26](#_Toc99640150)

[Distribución 26](#_Toc99640151)

[Disponibilidad 26](#_Toc99640152)

[Mantenimiento de los Procedimientos Actualizados 26](#_Toc99640153)

[11. ACTIVIDADES PERMANENTES PARA LA RECUPERACIÓN 27](#_Toc99640154)

[12. HISTORIAL DE CAMBIOS 29](#_Toc99640155)

[13. APROBACIÓN 29](#_Toc99640156)

# INTRODUCCIÓN

El DRP, Plan de Recuperación de Desastres, por sus siglas en inglés (Disaster Recovery Plan), es el documento que establece formalmente las medidas que se deben tomar al interior de la organización, desde los puntos de vista Operacional, Organizacional y de las Tecnologías de la Información (TI), para proteger los datos y los recursos tecnológicos que soportan la ejecución y la continuidad de los procesos críticos de negocio.

Este documento busca establecer el modo como el Ministerio de Hacienda y Crédito Público (MHCP) enfrentará la ocurrencia de un desastre que amenace la disponibilidad de los recursos y servicios tecnológicos críticos para la continuidad de los procesos de negocio.

# OBJETIVOS

# OBJETIVO GENERAL

Minimizar la posible pérdida financiera, reputacional y operativa ante un evento inesperado, previendo procedimientos de recuperación efectivos y eficientes. Así mismo, reducir las consecuencias de la posible pérdida de información relacionada con el evento inesperado a un nivel aceptable al ejecutar procedimientos de prevención, respuesta y recuperación apropiados.

Para la República de Colombia es de suma importancia y de gran valor que el MHCP cuente con un Plan de Recuperación de Desastres (DRP), esto dado que sus procesos son críticos para la operación de todos los sectores del país y en especial para su desarrollo.

El Plan de Recuperación de Desastres (DRP) permitirá mantener la continuidad de los servicios tecnológicos que soportan los procesos críticos de negocio, cuando la organización deba enfrentar situaciones de eventos de diferente naturaleza o tipología y a su vez, permitirá minimizar el impacto negativo que pudiese llegar a tener la misma frente a terceros.

# OBJETIVOS ESPECÍFICOS

Este **DRP** fue desarrollado para alcanzar los siguientes objetivos específicos:

* Dar continuidad a los servicios tecnológicos críticos del MHCP en caso de presentarse una situación de contingencia mayor o catastrófica.
* Disponer de un plan que oriente la coordinación de actividades a ejecutar por parte del personal del área de tecnología del Ministerio y los Proveedores Externos de servicios tecnológicos críticos para el negocio, ante la ocurrencia de un evento que amerite la activación del DRP de acuerdo con los Análisis de Impacto de negocio (BIA con sus siglas en inglés Bussiness Impact Analysis), en los cuales se evidencia que un amplio porcentaje de los procesos más críticos de la entidad se soportan en servicios tecnológicos.
* Fortalecer la planeación del manejo de eventos críticos y la debida articulación con las instancias establecidas en el esquema de gobierno del SGCN de la Entidad.
* Recuperar las aplicaciones críticas del negocio de una manera oportuna, incrementando la habilidad de la entidad para recuperarse de una pérdida o daños a las instalaciones y servicios.
* Administrar exitosamente el desastre, minimizando el impacto al negocio.
* Gestionar adecuadamente las comunicaciones ante la ocurrencia de evento críticos.

# TERMINOS Y DEFINICIONES

Se aclaran los conceptos claves que se requieren tener para poder entender el desarrollo del Plan de Recuperación de Desastres (DRP).

**AMENAZA:** Evento que constituye una posible causa de riesgo o perjuicio para alguien o algo

**ANÁLISIS DE RIESGOS:** Corresponde al examen minucioso, acucioso, diligente y cuidadoso que se efectúa con un método establecido para analizar las amenazas y/o vulnerabilidades en el negocio de una organización con el fin de poder establecer las posibles pérdidas y/o daños basados en la probabilidad de ocurrencia de los riesgos. El objetivo del análisis de riesgos es valorar el grado de aceptación de cada riesgo para el negocio.

**AZURE:** Plataforma de nube de Microsoft

**BD:** Base de Datos.

**BIA:** Siglas en inglés (Bussiness Impact Analisys) de Análisis de Impacto de Negocio

**CDA**: Centro de Datos Alterno. Para los efectos de este documento se puede mencionar como Sitio Alterno.

**DESASTRE**: Cualquier evento accidental, natural o intencional que amenaza o interrumpe las operaciones o servicios normales de TI por un período de tiempo que afecta significativamente *a la organización, por eventuales* pérdidas irreparables o la interrupción del negocio

**DNS:** Servidor de Nombres de Dominio

**DRP:** Plan de recuperación de desastre, es un proceso documentado o conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre.

**IMPACTO:** Conjunto de los posibles efectos negativos producto de la ocurrencia de un riesgo.

**MHCP:** Ministerio de Hacienda y Crédito Público.

**PROCESOS CRITICOS:** Corresponden al conjunto de actividades que han sido definidas como importantes para la operación de una organización en las que no debe ser permitida ni la más mínima perdida de su continuidad y/o disponibilidad.

**RIA:** Análisis de Riesgos de Interrupción

**RIESGO:** Posibilidad de que algo suceda o no.

**PUNTO OBJETIVO DE RECUPERACIÓN (RPO):** Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

**PUNTO TIEMPO OBJETIVO DE RECUPERACIÓN (RTO):** Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

**SGCN**: Sistema de Gestión de Continuidad del Negocio

**SITIO ALTERNO:** Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción. Para el caso del MHCP, la ubicación puede referirse a instalaciones físicas y/o plataformas en la nube.

**VULNERABILIDAD:** Cualquier debilidad, carencia, falencia, acción desacertada o equivocada, que se presente en la operación del negocio, y en especial la susceptibilidad del negocio para que sea atacado por alguna amenaza. Ha de aclararse que una vulnerabilidad puede existir o hallarse independientemente de cualquier amenaza existente.

# ALCANCE

Las actividades de los equipos de recuperación se dividen en actividades de preparación y actividades de respuesta y recuperación.

El DRP (Disaster Recovery Plan o Plan de Recuperación de Desastres), formula las actividades y lineamientos que deben ser considerados por el MHCP, para recuperar los servicios y recursos tecnológicos que dan soporte a sus procesos **críticos** de negocio, ante la ocurrencia de algún evento que pueda afectar su normal funcionamiento y se indican los puntos de articulación con los aspectos establecidos en el esquema de gobierno del SGCN del MHCP.

En concordancia con lo anterior el Anexo *Servicios y/o Sistemas Críticos DRP - MHCP* adjunto a este documento, establece los servicios que serán cubiertos por el Plan de Recuperación de Desastres (DRP)

Se establecen igualmente en este documento las actividades de preparación (actividades de carácter preventivo) que deben realizarse de manera permanente, de forma que se propenda en todo momento por la adecuación tanto de las actividades como de los recursos, a las necesidades cambiantes de la entidad, de cara a la ocurrencia de un evento que derive en impactos de importancia en los servicios TIC de la Entidad.

# ANALISIS Y JUSTIFICACIÓN DEL PLAN

La necesidad de desarrollar el DRP está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios de TI que soportan procesos críticos de negocio, en virtud de la ocurrencia de alguna situación crítica interna o externa, que impida el acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo por un período inaceptable de tiempo.

**El plan se basa en los resultados del análisis BIA de los procesos de la entidad** y la identificación regular de los riesgos potenciales a los cuales están expuestos los datos y los recursos tecnológicos que soportan la ejecución y la continuidad de los procesos críticos de negocio del MHCP, a partir de los cuales se establecen los efectos de un eventual desastre, con el propósito de determinar los aspectos de la estrategia y medidas que deben adelantarse para llevar a cabo la recuperación de la operación en el menor tiempo posible, de acuerdo con los requerimientos de negocio de la entidad.

A partir de los anteriores análisis, se establecen los objetivos de recuperación para cada uno de los procesos de negocio, los cuales implican los mismos objetivos de recuperación para los sistemas de información que los soportan mediante los siguientes indicadores:

* **Tiempo de Recuperación Objetivo (RTO - Recovery Time Objective):** Es el tiempo que el proceso puede estar interrumpido sin ocasionar mayores impactos al logro de sus objetivos. Es el plazo en el cual queremos ver recuperado el proceso.
* **Punto de Recuperación Objetivo (RPO - Recovery Point Objective):** Es la pérdida máxima tolerable de datos. Si se pierden más datos, su reconstrucción es compleja, demorada o no se puede llevar a cabo.
* **Periodo Máximo Tolerable de Interrupción (MTPD - Maximum Tolerable Period of Disruption):** Es el tiempo máximo que puede estar interrumpido el proceso. Si no se logra la recuperación en dicho periodo, los impactos sobre la imagen institucional, la operación y los objetivos del proceso se traducen en pérdidas mayores. El MTPD debe ser mayor al RTO estimado.

Pantalla de video juego

Descripción generada automáticamente con confianza media

Ilustración 1. Línea de Tiempo RRPO, RTO y MTPD

El Anexo *Servicios y/o Sistemas Críticos DRP - MHCP* adjunto a este documento, presenta los RTO (franjas de recuperación) definidos para los servicios TI críticos de acuerdo con los resultados obtenidos de los análisis antes mencionados.

Cabe señalar que previo a la recuperación de cualquier sistema funcional, se requiere activar los servicios tecnológicos de base que se relacionan a continuación, sin los cuales no sería posible el funcionamiento de los primeros:

* DNS externos
* Controladores de Dominio
* FireWalls
* Terminadores de VPN SSL
* Balanceadores de Carga F5

Concluyendo, el plan busca que la eficiencia en la recuperación de un desastre se determine por el desempeño colectivo con el fin de preservar la integridad de los procesos del negocio y defender los bienes e intereses de la Nación que le fueron entregados al Ministerio de Hacienda y Crédito Público (MHCP).

Finalmente cabe destacar como elemento central de la estrategia de recuperación de los servicios TI el Centro de Datos Alterno, denominado también Sitio Alterno, el cual constituye el soporte principal del Plan de Recuperación de Desastre (DRP) por alojar un espejo de los servicios TI que soportan los procesos y funciones críticas para la entidad.

# ESTRATEGIA GENERAL DE RECUPERACIÓN

Las estrategias a seguir serán acordes a la magnitud y duración estimada del incidente y se deberán tomar en cuenta los siguientes aspectos:

* Evaluación de los daños
* Evaluación del tiempo estimado de la recuperación
* Análisis exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo con el tipo de incidente.

Así mismo y en concordancia con lo anterior se deben contemplar en las estrategias los siguientes momentos:

* Evaluación de daños
* Activación Sitio Alterno
* Retorno sitio principal

# ANÁLISIS Y EVALUACIÓN DE DAÑOS

Como parte de las estrategias inmediatas ante una posible crisis, se indican a continuación y de forma general, las tareas que deben efectuarse lo más rápido posible, cuando se reporta un incidente o evento potencialmente catastrófico

1. Evaluación inicial del alcance del incidente y fallos – Busca identificar el estado de los componentes de la infraestructura tecnológica y de los servicios TI, determinando lo siguiente:
   * 1. Si la infraestructura es rescatable.
     2. Si la infraestructura es utilizable.
     3. Si la infraestructura es reparable.
     4. Si hay pérdida total del equipo.
2. Evaluar el estado del Centro de cómputo.
3. El personal del centro de cómputo siempre que sea posible efectuará inmediatamente respaldos de emergencia y procedimientos de apagado de los equipos.
4. Validar la criticidad de la falla (Contingencia menor, mayor o catastrófica) tomando en consideración el análisis de la magnitud del incidente observado de acuerdo con lo señalado en la siguiente tabla

| Nivel de Incidencia | Descripción | Ejemplo |
| --- | --- | --- |
| Menor | En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de detección, diagnóstico y reparación de fallas, activando los procedimientos de atención de problemas utilizados día a día por el personal del Ministerio de Hacienda y Crédito Público. | Caída de un servicio por la desconexión o apagado no previsto de un dispositivo de comunicaciones, el incidente puede ser detectado y resuelto en muy poco tiempo sin necesidad de declarar una contingencia. |
| Mayor | De presentarse una incidencia mayor en los equipos y sistemas del centro de cómputo principal que impida la función general de la entidad, esta deberá ser identificada y corregida a la brevedad.  Si el tiempo estimado de reparación que determinen los equipos de recuperación responsables de las aplicaciones o recursos técnicos críticos, es superior al tiempo identificado para que esté operativo, el Líder de Recuperación del DRP decidirá sobre la pertinencia de activar el Plan DRP.  En este caso, el Líder de Recuperación Tecnológica deberá evaluar la situación de cara al RTO y RPO de los procesos afectados y determinar si se debe activar o no el DRP. | Caída de varios servidores por fallas en el fluido eléctrico y luego de la caída uno o varios de los servicios críticos de TI no pueden ser levantados por daños en las bases de datos, en las aplicaciones o en los servidores y se requiere el restablecimiento de una copia de seguridad que puede tomar entre 2 y 6 horas. |
| Catastrófica | Se refiere a la situación en la cual se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa las operaciones del Ministerio de Hacienda y Crédito Público en sus instalaciones ubicadas en el Edificio San Agustín en la Carrera 8va. 6-64 y la sede de Casas Santabárbara en la Carrera 7ª # 6B- 80 de la ciudad de Bogotá.  Este escenario conlleva la necesidad de activar el Plan. | Un ejemplo de un incidente catastrófico puede ser la afectación grave del centro de datos principal por inundaciones, incendios, ataques cibernéticos o eventos naturales que impliquen la destrucción o inhabilitación parcial o total de componentes críticos de TIC. |

Tabla 1. Tipificación de Incidentes

Así mismo y a modo de referencia, el anterior análisis puede complementarse con la revisión de los posibles escenarios de desastre que pueden ocurrir. En **Anexo #1** de este documento se incluye una clasificación y descripción de dichos escenarios.

**Nota:** En caso de que la contingencia haya sido detectada por el personal de Tecnología, se deberá e informar al Líder y / o Coordinador DRP, sobre el incidente:

1. Fecha en que se espera que el servicio sea restablecido, de lo contrario, proporcionar fecha probable en que se conocerá el estado en el que se encuentra el servicio;
2. Fecha y hora en que sus aplicaciones serán restablecidas, si se tiene conocimiento de ello, de no ser así, indicar la fecha tentativa del restablecimiento de estos.

A partir de la anterior información, generar las recomendaciones respectivas sobre la necesidad de activar el DRP

# ACTIVACIÓN DEL DRP

Las estrategias y planes de acción considerados para la recuperación de los servicios tecnológicos del Ministerio de Hacienda y Crédito Público están orientados a gestionar cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal al edificio donde se ubica el centro de cómputo o bien a los servicios de cómputo y telecomunicaciones en que se apoyan las aplicaciones críticas de la entidad.

Este plan podrá ser activado únicamente cuando el Líder de Recuperación Tecnológica lo indique por recomendación del equipo de evaluación de daños y sea aprobado por el Líder de Continuidad de Negocio

La Activación comprende el desarrollo de las siguientes actividades, las cuales son explicadas con mayor detalle en el numeral

1. Ejecución Procedimientos de recuperación
2. Monitoreo y Seguimiento a los servicios que quedan operando en contingencia
3. Comunicación continúa interna/externa a involucrados
4. Activación de plan de retorno de contingencia
5. Declaración de fin de contingencia
6. Regreso a modo normal de operación
7. Notificación formal de fin de contingencia
8. Fin de Contingencia

# MECANISMOS DE COMUNICACIÓN

Para las notificaciones es necesario ajustarse al esquema definido en la sección *“12. Gobierno de Continuidad de Negocio y Árbol de Llamadas”* del documento *“Plan de Continuidad de Negocio MHCP”.*

No obstante, lo anterior, en caso de que no haya disponibilidad de los medios de comunicación establecidos, se debe priorizar la realización de la comunicación por el medio más eficiente que se tenga a disposición.

# EQUIPO DE RECUPERACIÓN

# ESTRUCTURA

Dentro del Plan de Recuperación de Desastres (DRP), una práctica recomendada es la creación de equipos de trabajo que desempeñan grupos de funciones y a su vez tendrán responsabilidades específicas dentro del Plan.

La siguiente ilustración muestra la organización establecida al interior de la Dirección de Tecnología para ejercer su rol de Equipo Líder de Recuperación Tecnológica dentro del SGCN del MHCP.

Ilustración 2. Equipos de contingencia

# LÍDER DRP (LÍDER DE RECUPERACIÓN TECNOLÓGICA)

Forma parte del Equipo Directivo de Continuidad de Negocio. Audita que el plan se ejecute de acuerdo con lo plasmado en los documentos del plan.

Notifica las decisiones tomadas por el Equipo Directivo del SGCN.

Es informado lo antes posible de cualquier incidente crítico para solicitar la toma de decisiones efectivas encaminadas a la superación de eventos que puedan afectar la continuidad de los servicios tecnológicos incluidos en el alcance de este plan.

.

Interfaz de usuario gráfica

Descripción generada automáticamente

Ilustración 3. Líder del DRP

# EQUIPO EVALUADOR DE DAÑOS

Valida los daños a la infraestructura de TIC con el fin de determinar la afectación y poder informar al Líder del DRP el estado del servicio, para determinar si se debe declarar una contingencia. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento en el que haya evidencia o sospecha de daños físicos, técnicos o lógicos en uno o más de los componentes de la infraestructura de TI.

Entre las actividades que debe desarrollar este equipo se cuentan las siguientes:

* Identificar daños en la infraestructura física
* Identificar daños a equipos tecnológicos
* Identificar daños en redes eléctricas y de comunicaciones
* Determinar si las instalaciones, los equipos y las redes se encuentran en condiciones adecuadas para su funcionamiento
* Identificar e informar los recursos requeridos para la restauración de los servicios y las operaciones

Ver anexo Formato de Evaluación de Daños.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Ilustración 4. Equipo Evaluador de Daños

# EQUIPO COORDINADOR DE DRP

Recibe la solicitud de activación del Plan de Recuperación de Desastres por parte del Comité Directivo de DRP del Ministerio de Hacienda e inicia la ejecución de las acciones que correspondan para superar la situación de contingencia.

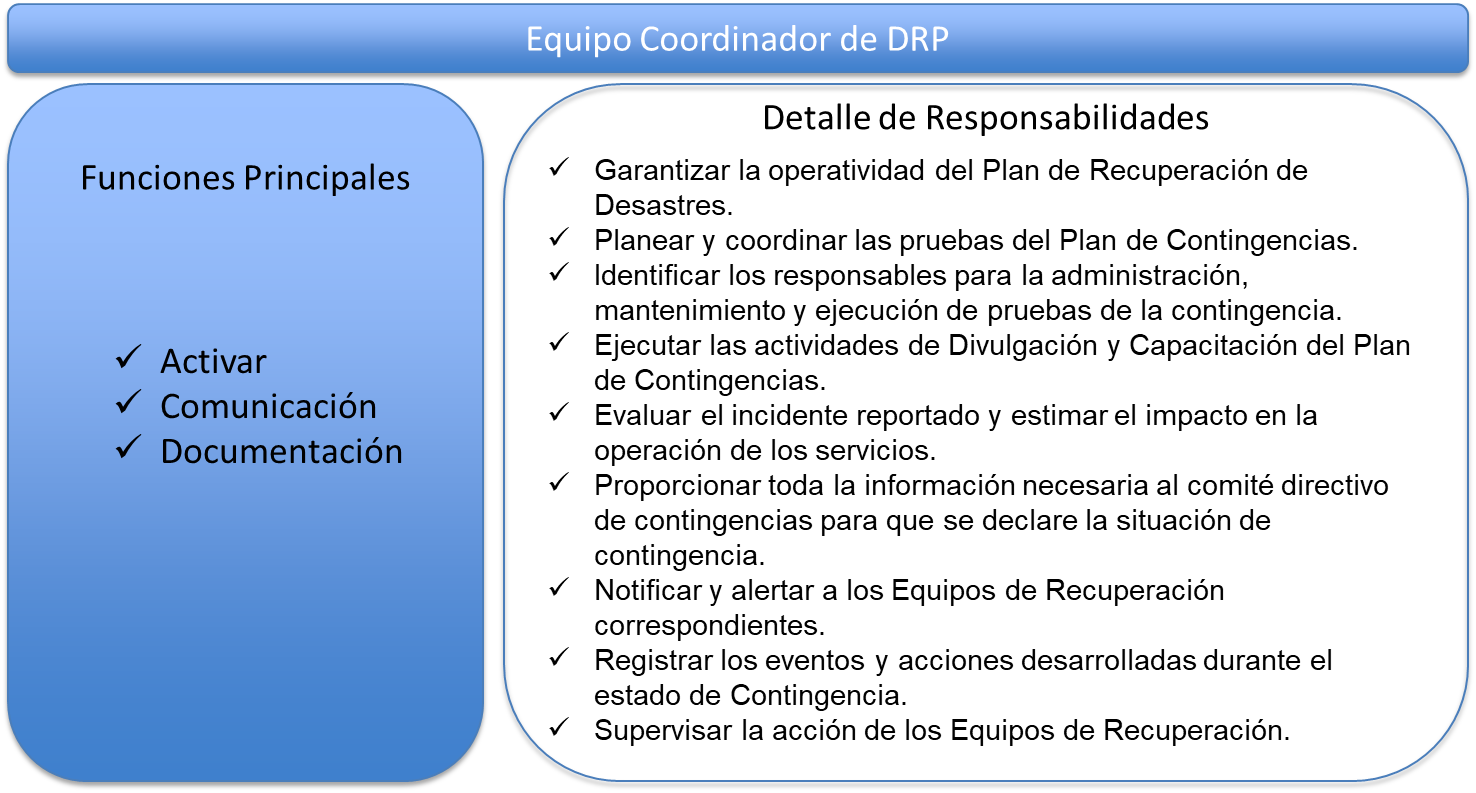


Ilustración 5. Equipo Coordinador de DRP

# COORDINADOR DE CENTRO DE DATOS ALTERNO

Recibe la solicitud de activación del Plan de Recuperación de Desastres por parte del Comité Directivo de DRP del Ministerio de Hacienda e inicia la ejecución de las acciones que correspondan para la superar la situación de contingencia.

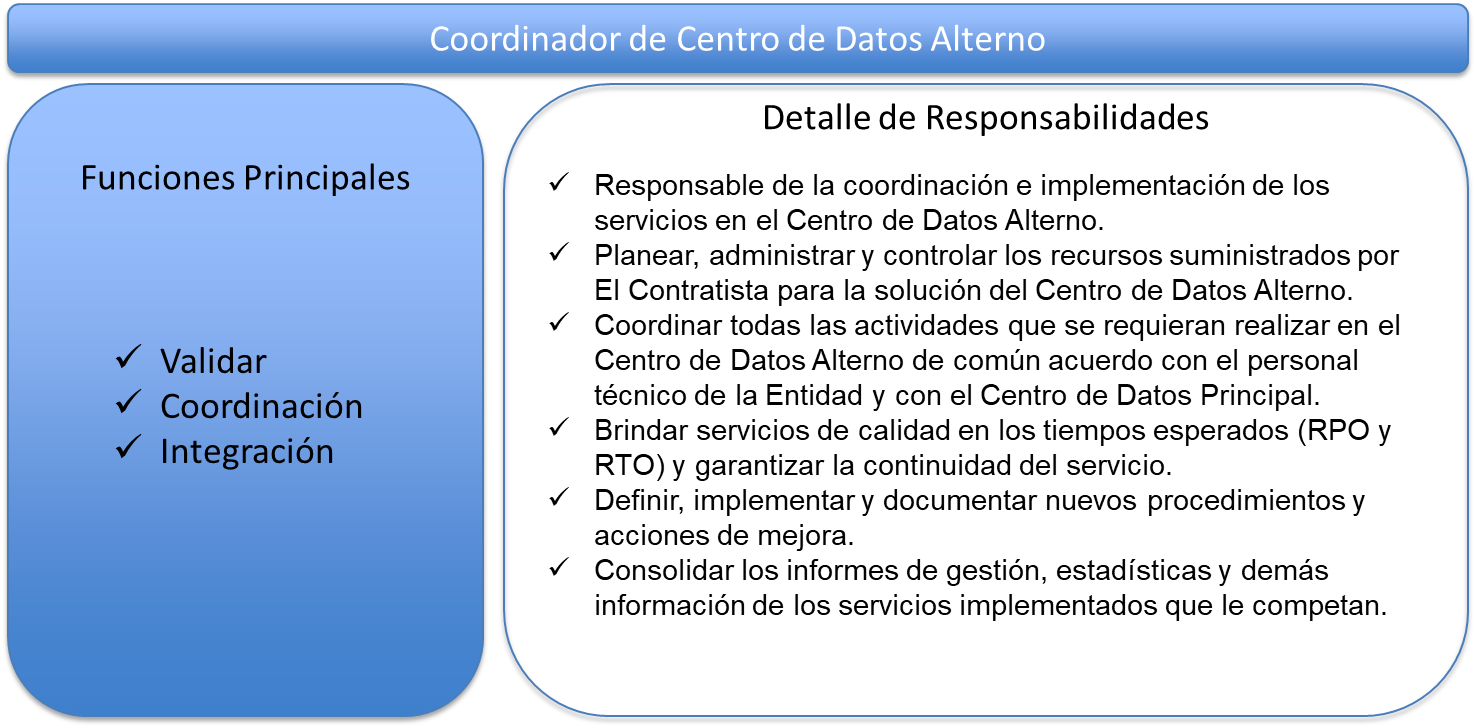


Ilustración 6. Coordinador del Centro de Datos Alterno

# EQUIPO DE RECUPERACIÓN DE DRP

El equipo de recuperación de contingencias está compuesto por el equipo de Especialistas del MHCP y la firma proveedora de servicios Sitio Alterno y el Equipo de Soporte del Cetro de Servicios Tecnológicos - CST .

Recibe la solicitud de activación del Plan de Recuperación de Desastres del Equipo Coordinador de DRP y se encarga de restablecer la operación de los servicios de hardware, software, telecomunicaciones, energía y seguridad física que dificulten la continuidad de la operación en el sitio principal.



Ilustración 7. Equipo de Recuperación de DRP

Dentro del equipo de Recuperación de Contingencias, el equipo de Soporte a Usuarios debe brindar el soporte a los usuarios finales del Ministerio de Hacienda para el desarrollo de sus actividades tareas durante el tiempo que esté operativa la contingencia.

El equipo de soporte a usuarios está conformado por:

* Coordinador del Centro de Servicios Tecnológicos del MHCP
* Soporte Nivel I y II del Centro de Servicios Tecnológicos
* Operadores de Centros de Datos Alterno

**Responsabilidades:**

* Conocer y entender el Plan de Contingencia.
* Verificar con los usuarios finales del MHCP la estabilidad de las aplicaciones y reportar anomalías. Cooperar con el Equipo de Recuperación de Contingencias en la puesta en marcha del Plan de Contingencia.
* Verificar con los usuarios finales del MHCP la estabilidad de las aplicaciones y reportar anomalías. Actualizar los procedimientos existentes en el Manual de Contingencias que esté relacionado con su trabajo.

# LINEA DE SUCESIÓN

La línea de sucesión identifica los responsables asignados a los diferentes roles del DRP y sus alternos en caso de que estos no puedan asumir las actividades y/o tareas.

Estas personas fueron asignadas de acuerdo con los roles y responsabilidades que en la actualidad ejecutan. El detalle de la línea de sucesión para el equipo del DRP se presenta en el formato *Est.1.4.SGCN. Man.1 Fr.3 Relación de equipo de recuperación*.

# ÁRBOL DE LLAMADAS

El árbol de llamadas representa la cadena de llamadas que se debe seguir y cumplir para comunicar a los integrantes del DRP la activación del plan. Esta se ejecuta después de la declaración de contingencia realizada por el Líder del DRP.

El árbol de llamadas está dividido en equipos o grupos para permitir llamar a los integrantes requeridos según el tipo de contingencia que se haya declarado.

Tomando en cuenta la Ilustración *5. Equipos de contingencia*, cada nivel está encargado de llamar al nivel inferior según la estructura del plan y el llamado a cada integrante debe ser verificado por el nivel superior.

El director de Tecnología es el disparador de llamadas y responsable de la intercomunicación con el primer nivel de llamadas. A su vez, cada persona que desempeña un rol que incluya roles dependientes, tiene el deber de comunicar al nivel inferior el evento que le fue informado.

El llamado a los integrantes del plan se debe realizar siguiendo el procedimiento de comunicación necesario y utilizando los medios disponibles para realizarlo.

Cuando se presente un desastre, interrupción o evento contingente, se debe aplicar la siguiente cadena de llamadas:

| Rol | Responsabilidad | Medio Comunicación (\*) |
| --- | --- | --- |
| Líder de continuidad de negocio | Solicitar al Líder del DRP evaluar daños. | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder DRP | Comunicar al equipo evaluador la situación. | **Opción 1**: Reunión virtual mediante herramienta institucional.  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Equipo evaluador | Examinar la situación. |  |
| Equipo evaluador | Comunicar al Líder del DRP, el resultado del análisis de la evaluación de los daños. | **Opción 1**: Reunión virtual mediante herramienta institucional.  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder DRP | Comunicar al Líder de Continuidad de Negocio los resultados de la evaluación y realizar las respectivas recomendaciones. | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder de continuidad de negocio | Comunica decisión respecto a la aprobación de la activación del DRP | **Opción 1**: Reunión virtual mediante herramienta institucional.  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
|  | Si se decide activar DRP continua a la siguiente de lo contrario va a FIN CONTINGENCIA. |  |
| Líder DRP | Comunicar la decisión de activación del DRP al coordinador del DRP-MHCP y dar las instrucciones que considere relevantes para la activación del DRP | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder de coordinación del DRP-MHCP | Contactar al líder de coordinación del DRP de la firma de prestadora de los servicios de Sitio Alterno y dar las instrucciones que considere relevantes para la recuperación de los servicios en sitio alterno. | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder de coordinación del DRP-MHCP | Contactar a los proveedores de servicios tercerizados y dar las instrucciones que considere relevantes para la recuperación de los servicios que administra en sitio alterno dispuesto para tal fin. | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder de coordinación del DRP de la firma de prestadora del servicio de Sitio Alterno | Contactar a los integrantes del equipo de recuperación. (Especialistas MHCP, usuarios, contratistas) y orientar y controlar la ejecución de las labores de recuperación de los servicios en sitio alterno de acuerdo con las franjas de recuperación establecidas | **Opción 1**: Reunión virtual mediante herramienta institucional.  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Proveedores de servicios tercerizados | Gestionar la ejecución de las labores que sean requeridas para la normalización de la operación soportada en el servicio que administra de acuerdo con las necesidades de la entidad. | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder de coordinación del DRP de la firma de prestadora | Comunicar al Líder de coordinación del DRP-MHCP la recuperación de los servicios | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Proveedores de servicios tercerizados | Comunicar al Líder de coordinación del DRP-MHCP la recuperación de los servicios | **Opción 1**: Telefonía institucional  **Opción 2**: Mensajería institucional  **Opción 3**: otros medios disponibles y adecuados a la situación |
| Líder Recuperación Tecnológica | Declaración de fin de contingencia |  |
| Líder DRP MHCP | Coordinar regreso a modo normal de operación |  |
| Líder Recuperación Tecnológica | Notificación formal de fin de contingencia | * Mensajería institucional * Carteleras digitales * Intranet |
|  | **FIN CONTINGENCIA** |  |

Tabla 2. Árbol de llamadas

El anterior mecanismo de “**ARBOL DE LLAMADAS”** deberá ser utilizado por el equipo de recuperación de contingencia al momento de ser oficialmente informado del desastre.

El Coordinador del DRP y los líderes de los equipos de recuperación DRP mantendrán una coordinación y comunicación constante sobre las respuestas y acciones del incidente y las actividades de recuperación.

# PROCEDIMIENTO DE ACTIVACIÓN Y RETORNO DE SERVICIOS

Se describe a continuación, el proceso que se debe surtir desde que se activa la gestión del plan, previa notificación del desastre, hasta el momento en que el servicio es restaurado en el Sitio Principal en producción:

| Actividad | Descripción | Participantes |
| --- | --- | --- |
| Declaración de contingencia | El líder del SCNG solicita aprueba e instruye sobre la activación del DRP | Líder de la SGCN declara la contingencia |
| Establecer servicios a recuperar | Consiste en establecer cuáles son los servicios para recuperar y el orden en que debe realizarse la recuperación | Coordinador la activación del DRP |
| Informar a coordinadores DRP | Comunicar la necesidad de recuperar servicios en el Sitio Alterno a:   * Grupo de recuperación MHCP * Coordinador DRP – operador contratista sitio alterno * Coordinador DRP – Servicios Tercerizados | Coordinador la activación del DRP-MHCP |
| Ejecutar actividades de recuperación de servicios | Cada miembro de los equipos de recuperación tecnológica realiza las tareas que le corresponden en el sitio alterno, de acuerdo con lo establecido en la lista de chequeo definida para cada servicio. | Especialistas de recuperación |
| Realizar pruebas funcionales previas | Ejecutan pruebas de los servicios recuperados para verificar su correcto funcionamiento previo | Usuarios líderes de los servicios recuperados |
| Informar a Coordinador DRP-MHCP | Comunican el correcto funcionamiento de los servicios | Usuarios líderes de los servicios recuperados |
| Informar a Líder de recuperación tecnológica | Comunica el correcto funcionamiento de los servicios recuperados | Coordinador DRP-MHCP |
| Informar a Líder de SGCN | Comunica el correcto funcionamiento de los servicios recuperados | Líder de recuperación tecnológica |
| Solicitar comunicación | Solicita al Grupo de comunicaciones la divulgación a los usuarios de los sistemas, sobre el correcto funcionamiento de los servicios recuperados | Líder de SGCN |
| Informar disponibilidad servicios | Comunicar a los usuarios la disponibilidad de los servicios recuperados | Grupo de comunicaciones |
| Informar a Líder de SGCN | Informar sobre la disponibilidad de sitio principal para restaurar los servicios en dicho sitio | Líder de recuperación tecnológica |
| Aprobar activación sitio principal | Aprueba regresar al sitio principal | Líder de SGCN |
| Solicitar retorno al sitio principal | Informar al coordinador DRP-MHCP la aprobación del retorno al sitio principal | Líder de recuperación tecnológica |
| Informar a coordinadores DRP y demás especialistas | Comunicar la instrucción de retornar al sitio principal:   * Grupo de recuperación MHCP * Coordinador DRP – operador contratista sitio alterno   Coordinador DRP – Servicios Tercerizados | Coordinador la activación del DRP-MHCP |
| Ejecutar actividades de retorno al sitio principal | Cada miembro de los equipos de recuperación tecnológica realiza las tareas que le corresponden para reactivar los servicios en el sitio principal de acuerdo con lo establecido en la lista de chequeo definida para cada servicio. | Especialistas de recuperación |
| Realizar pruebas funcionales previas | Ejecutan pruebas de los en el sitio principal verificar su correcto funcionamiento previo | Usuarios líderes de los servicios recuperados |
| Informar a Coordinador DRP-MHCP | Comunican el correcto funcionamiento de los servicios | Usuarios líderes de los servicios recuperados |
| Informar a Líder de recuperación tecnológica | Comunica el correcto funcionamiento de los servicios restaurados en el sitio principal | Coordinador DRP-MHCP |
| Informar a Líder de SGCN | Comunica el correcto funcionamiento de los servicios restaurados en el sitio principal | Líder de recuperación tecnológica |
| Solicitar comunicación | Solicita al Grupo de comunicaciones la divulgación a los usuarios de los sistemas, sobre el correcto funcionamiento de los servicios restaurados en el sitio principal | Líder de SGCN |
| Informar disponibilidad servicios | Comunicar a los usuarios la disponibilidad de los servicios restaurados en el sitio principal | Grupo de comunicaciones |
| FIN PROCEDIMIENTO |  |  |

Tabla 3. Plan de Activación de Contingencia

# PLAN DE PRUEBAS DEL SITIO ALTERNO

La fase de pruebas debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro. Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera. Es también importante que las pruebas se lleven a cabo por las personas que serán responsables de esas actividades en una crisis.

Las pruebas deben ser periódicas para cada uno de los servicios y se deben ejecutar por lo menos una (1) vez al semestre. Las pruebas también se deben poder ejecutar cada vez que la entidad lo requiera.

El objetivo de estas pruebas es verificar la funcionalidad y configuración de los equipos y servicios ofrecidos y poder verificar la funcionalidad de los procedimientos internos de la Entidad en el momento de una contingencia. Cada una de las pruebas debe quedar documentada con su respectiva evidencia.

# TIPO DE PRUEBAS

* **TECNICAS:** Objetivo medir la correcta configuración y funcionamiento de la infraestructura del DRP y detectar errores en la configuración de las máquinas del CDA. [¿???]
* **FUNCIONALES:** Objetivo es validar el correcto funcionamiento y tiempos de respuesta de las aplicaciones y servicios implementados en la contingencia, tomando en cuenta lo siguiente:
* El resultado de cada caso de prueba debe ser igual al resultado de salida esperado.
* Encontrar fallas al ejecutar los diferentes casos de pruebas.
* La aplicación responde en los tiempos esperados.
* La aplicación cumple con los requerimientos mínimos para el funcionamiento

Ilustración 8. Fases del Plan de Pruebas

# FRECUENCIA DE LAS PRUEBAS

Las pruebas tendrán una recurrencia de ejecución semestral o cuando se ejecute algún cambio en la infraestructura o arquitectura actual de la entidad, con el fin de garantizar que el CDA este actualizado.

# RESULTADOS Y EVALUACION DE LAS PRUEBAS

De acuerdo con los resultados de las pruebas ejecutadas se deben medir los siguientes criterios:

* Tiempo: Tiempo transcurrido en la ejecución de las actividades definidas en el plan de Pruebas.
* Cantidad: De trabajo que los recursos emplean para la ejecución del plan de pruebas.
* Exactitud: De cada una de las actividades realizadas.

Las pruebas de recuperación de desastres deben realizarse de modo habitual. Las comunicaciones, la recuperación de datos y la recuperación de aplicaciones suelen ser los ejes de todas las pruebas de recuperación de desastres. La ejecución de estas pruebas nos permite medir los objetivos de la organización sobre el punto de recuperación (RPO) y el tiempo de recuperación (RTO).

# COORDINACIÓN CON LAS ÁREAS USUARIAS

Previo a la ejecución de las pruebas debe definirse/tratarse con el (las) áreas usuarias, los siguientes aspectos:

* Fecha y hora de activación en Sitio Alterno y Fecha y hora de regreso a Sitio Principal
* La forma en que se llevaran a cabo la prueba
* Los riesgos asociados
* Los resultados esperados

# DISTRIBUCIÓN, DISPONIBILIDAD Y MANTENIMIENTO DEL PLAN

Las responsabilidades de mantenimiento, disponibilidad y distribución del plan de recuperación de desastres, están a cargo del Coordinador DRP. Estas incluyen revisiones periódicas del plan, tomando en consideración los requerimientos del negocio, las estrategias de recuperación y la capacitación del personal.

## Distribución

La documentación soporte de este plan se encontrará ubicada en la ruta \\minhacienda\cedin\DT\DRP del servidor de archivos y podrá ser consultada vía intranet en el sitio principal y a través de conexión segura (VPN – Virtual Private Network) en sitio alterno.

## Disponibilidad

Todos los integrantes de los equipos de recuperación de contingencia tienen acceso garantizado a la última copia actualizada del plan a través de los diferentes medios y sitios autorizados.

## Mantenimiento de los Procedimientos Actualizados

Hay que asegurar que el plan de recuperación de desastres, incluyendo todos los recursos y procedimientos identificados se mantiene en un estado de actualización constante.

Así mismo el Coordinador DRP-MHCP tiene a su cargo las siguientes responsabilidades:

1. Asegurarse que todos los integrantes de los equipos de recuperación y sus suplentes tengan acceso al plan actualizado.
2. Asegurarse que todo el personal del equipo de recuperación considera su experiencia aplicable, para la recuperación de sus operaciones como parte de sus tareas normales.
3. Asegúrese que todos los respaldos de información y actividades de rotación de información de registros vitales están siendo efectuados.
4. Dar mantenimiento al plan, mediante la actualización de la lista de servicios críticos, franjas de recuperación, integrantes del equipo de recuperación, guías de recuperación, listas de chequeo y demás documentos que soporten este plan, tomando en cuenta cualquiera de las siguientes circunstancias:
   * 1. Cualquier cambio de personal en el área que forma parte de los grupos de recuperación
     2. Cualquier cambio significativo a los requerimientos de recuperación.
     3. Cualquier cambio significativo a los procedimientos de recuperación, tales como la adición de un nuevo servicio.
5. 5. Participar sobre todo en el programa de pruebas del plan cuando sea requerido, se recomienda como mínimo dos (2) veces por año.

# ACTIVIDADES PERMANENTES PARA LA RECUPERACIÓN

Para que un equipo de recuperación funcione adecuadamente, se requiere seguir ciertos pasos sencillos, pero rutinarios con anticipación a lo que pueda suceder. Estas medidas preventivas se verifican y afinan con los procesos de pruebas.

El coordinador del DRP deberá ser responsable de tener los procedimientos actualizados, gestionar los recursos necesarios para la recuperación y que, ante la necesidad de recuperar los servicios alojados en el sitio alterno, se aplique lo establecido en este documento.

El coordinador del DRP y el equipo de recuperación de contingencia deberán tomar las medidas y acciones pertinentes para asegurar una recuperación exitosa, contando con los recursos disponibles para enfrentar cualquier incidente. Estas actividades deberán considerarse como tareas permanentes y los registros y la actualización de la documentación que soporta la gestión del DRP (ante cualquier cambio significativo en alguno de estos elementos o cuando los resultados de las pruebas así lo exijan), deben ser objeto de verificación al menos una vez al año.

Son tareas permanentes del equipo Coordinador del DRP-MHCP, las siguientes:

1. Asegurar la existencia y actualización de una lista de chequeo por cada servicio con el fin de poder revisar la funcionalidad del servicio en tanto en la contingencia como en el retorno a la normalidad.
2. Posterior a las contingencias asegurar que se realicen las siguientes tareas:

* Actualización del plan de recuperación de desastres
* Documentación de lecciones aprendidas
* Actualización Planes de Prueba

1. Asegurar que los cambios sobre los elementos que conforman el portafolio de servicios de TI sean documentados y sean incluidos en los procedimientos de recuperación y sean conocidos por los equipos de recuperación.
2. Asignar a un responsable por equipo de recuperación para que se encargue de actualizar los procedimientos de recuperación de los servicios que le competan.
3. Definir el procedimiento de comunicación entre los equipos de recuperación.
4. Obtener la información precisa para apoyar al Líder del DRP en la coordinación y la gestión de las actividades de recuperación.
5. Llevar de forma continua un programa de promoción/difusión sobre la importancia del Plan ante los equipos de recuperación.
6. Coordinar la capacitación de los integrantes de los equipos de recuperación, para actuar de acuerdo con el plan definido.
7. Supervisar continuamente, que el Centro de Datos Principal y el Centro Datos Alterno estén preparados según los requerimientos de recuperación.
8. Coordinar la realización de las pruebas.
9. Coordinar las reuniones de trabajo para establecer procedimientos de mantenimiento y actualización del plan.
10. Determinar los procedimientos de almacenamiento del plan y coordinar la distribución de este.
11. Hay que asegurar que los respaldos de la información crítica se ejecuten de acuerdo con las políticas de la Entidad.
12. Asignar un responsable de mantener actualizado el directorio de los equipos de recuperación.
13. Revisar y validar las estrategias y procedimientos de recuperación
14. Gestionar la realización de capacitaciones con los siguientes fines:

* Concientización Divulgación del plan mediante los siguientes mecanismos:
  + Documento escrito.
  + Intranet
  + Charlas / Conferencias.

* Entrenamiento en roles y responsabilidades.

La audiencia de las capacitaciones planeadas debe incluir a todos los miembros de los equipos de recuperación.

# HISTORIAL DE CAMBIOS

| **FECHA** | **VERSIÓN** | **DESCRIPCIÓN DEL CAMBIO** | **Asesor SUG** |
| --- | --- | --- | --- |
| 16/03/2022 | 1.0 | Se crea primera versión oficial del documento en el SUG a partir de versiones elaboradas/ajustadas en el marco de los contratos de servicios de sitio alterno y de la implementación del sistema de continuidad de negocio del MHCP realizada mediante consultoría con la firma Globaltek. | Sindy Julieth Tovar Torres |

# APROBACIÓN

|  |  |
| --- | --- |
| **ELABORADO POR:** | **Nombre:** Ma. Eugenia Chavez Robayo  **Cargo:** Asesor Despacho DT  **Dependencia:** Despacho DT  **Fecha:** 14 de febrero 2022 |
| **REVISADO POR:** | **Nombre:** Jaime Alberto Molina Suarez  **Cargo:** Asesor  **Dependencia:** Subdirección de Administración de Recursos Tecnológicos  **Fecha:** 14 de marzo 2022 |
| **APROBADO POR:** | **Nombre:** Ricardo Rios Rosales  **Cargo:** Director  **Dependencia:** Dirección de Tecnología  **Fecha:** 17 de marzo 2022 |

**ANEXO #1 – ESCENARIOS DE DESASTRE**

1. **DAÑOS SEVEROS EN EL DATACENTER PRINCIPAL**

La pérdida total o parcial de las instalaciones del Centro de Datos principal del Ministerio de Hacienda y Crédito Público, puede deberse a diferentes situaciones y/o motivos tales como:

* Conflictos armados internos o externos.
* Actos perpetuados por terroristas y/o grupos armados ilegales.
* Hostilidades u operaciones bélicas ya sea o no declarada una guerra.
* Rebelión, sedición, usurpación o retención ilegal del mando.
* Asonada, motín, o conmoción popular.
* Huelgas, conflictos colectivos de trabajo o suspensión de hecho de labores y por movimientos subversivos y/o acciones terroristas y/o de grupos armados ilegales que conlleven a daños materiales en las instalaciones.
* Deslizamientos de tierra y/o otros elementos, avalanchas, fallas geológicas, terremoto, temblor, asentamientos, inconsistencias del suelo, inundaciones, erupción volcánica, vientos o cualquier otra convulsión de la naturaleza.
* Reacción o radiaciones nucleares o contaminación radioactiva.

1. **CAÍDA DE CANALES DE COMUNICACIONES**

La pérdida total o parcial de los servicios de comunicaciones puede originarse en diferentes amenazas:

* Daños causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones llevadas a cabo con el propósito de dar cumplimiento a sus obligaciones.
* Por delitos por computador y/o medios electrónicos que puedan afectar las telecomunicaciones.
* Por exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, intercepción de líneas (wire-trapping), wardriving, dispositivos adosados (piggybacking), cierre de computadoras (shutdown), ataques de negación de servicio, redondeo hacia abajo, técnicas de salami, caballos de Troya, virus, gusanos y bombas lógicas que generen la pérdida total o parcial de los servicios de negocio.
* Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética, caída de intranet del Estado, caída de backbones que alteren y/o interrumpan el normal funcionamiento de los equipos que se utilicen para los procesos de negocio.
* Por acciones tomadas por personas que terminen en el sabotaje de los procesos de negocio a causa de chantaje, fraude, descontentos, huelgas, amenazas (acción disciplinaria o con despido), adictos y/o experimentación de problemas financieros o emocionales.
* Dolo y/o imprudencia manifiesta por parte de personas directa y/o indirectamente involucrada en los procesos de negocios que conlleven a la suspensión total o parcial de los servicios.
* Pérdida del hardware, software y data de propiedad y/o tenida a cargo, en custodia y/o control del Ministerio de Hacienda y Crédito Público.
* Pérdida o daño debido al cálculo o diseño erróneo del hardware y software.
* Falla y/o daño eléctrico interno o desarreglo de los equipos y dispositivos del centro de datos.
* Daños y/o fallas atribuibles a la falta y/o carencia de diligencia en los mantenimientos predictivos, preventivos y correctivos a los equipos y dispositivos del centro de datos.
* Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor, y/o los medios empleados para extinguir y/o contener un incendio ya sea por acción directa e inmediata del mismo, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.
* Por la combustión espontánea de algún elemento que forme parte de algún equipo y/o dispositivo del centro de datos.

1. **DAÑOS GRAVES EN SERVIDORES Y/O DISPOSITIVOS DE ALMACENAMIENTO**

* Daños causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones llevadas a cabo con el propósito de dar cumplimiento a sus obligaciones.
* Por la pérdida de aquellos bienes cuyo valor excede el de los materiales que los componen tales como planos, modelos, metodologías, documentos de cualquier clase, archivos magnéticos y/o cualquier otro medio de archivo computacional, que traiga como consecuencia que no se pueda efectuar la operación normal de los servicios del negocio.
* Por la reticencia u omisión de los procedimientos establecidos para la prestación de los servicios del negocio.
* Por delitos por computador y/o medios electrónicos que puedan afectar la prestación de los servicios del negocio.
* Por utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, la alteración de datos en forma no autorizada, la negación de la ocurrencia de un acción o transacción, la visualización de información no autorizada, la negación del servicio y/o operación de la(s) aplicación(es) y la obtención del acceso a la plataforma y/o a los aplicativos con todos los privilegios y/o roles que conlleven a la pérdida total o parcial de los servicios del negocio.
* Por las vulnerabilidades en sistemas operativos y/o en las aplicaciones que estén alojadas en el centro de datos.
* Por exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, intercepción de líneas (wire-trapping), wardriving, dispositivos adosados (piggybacking), cierre de computadoras (shutdown), ataques de negación de servicio, redondeo hacia abajo, técnicas de salami, caballos de Troya, virus, gusanos y bombas lógicas que generen la pérdida total o parcial de los servicios de negocio.
* Por exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios de negocio.
* Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética, caída de intranet del Estado, caída de backbones que alteren y/o interrumpan el normal funcionamiento de los equipos que se utilicen para los procesos de negocio.
* Por problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción / regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios de negocio.
* Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención/modificación indebida de información, y la inestabilidad del rendimiento del hardware y/o software que conlleve a la pérdida total o parcial de los servicios del negocio.
* Por acciones tomadas por personas que terminen en el sabotaje de los procesos de negocio a causa de chantaje, fraude, descontentos, huelgas, amenazas (acción disciplinaria o con despido), adictos y/o experimentación de problemas financieros o emocionales.
* Dolo y/o imprudencia manifiesta por parte de personas directa y/o indirectamente involucrada en los procesos de negocios que conlleven a la suspensión total o parcial de los servicios.
* Pérdida del hardware, software y data de propiedad y/o tenida a cargo, en custodia y/o control del Ministerio de Hacienda y Crédito Público.
* Pérdida o daño debido al cálculo o diseño erróneo del hardware y software.
* Falla y/o daño eléctrico interno o desarreglo de los equipos y dispositivos del centro de datos.
* Daños y/o fallas atribuibles a la falta y/o carencia de diligencia en los mantenimientos predictivos, preventivos y correctivos a los equipos y dispositivos del centro de datos.
* Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor, y/o los medios empleados para extinguir y/o contener un incendio ya sea por acción directa e inmediata del mismo, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.
* Por la combustión espontánea de algún elemento que forme parte de algún equipo y/o dispositivo del centro de datos.

1. **DIFICULTADES DE ACCESO A SISTEMAS DE INFORMACIÓN**

* Dificultades de conectividad
* Imposibilidad de acceso a equipos de trabajo
* Interrupción de funcionalidades y/o servicios provistos por terceros
* Cortes de servicios de transporte y/o comunicaciones