**INDICE**

[INTRODUCCIÓN 2](#_Toc41000772)

[1. TERMINOS Y DEFINICIONES 2](#_Toc41000773)

[2. OBJETIVO 4](#_Toc41000774)

[3. ALCANCE 5](#_Toc41000775)

[4. GENERALIDADES DEL PLAN DE CONTINGENCIA 5](#_Toc41000776)

[4.1. Estrategia general de recuperación 6](#_Toc41000777)

[4.2. Estrategia de acción 6](#_Toc41000778)

[4.3. Clasificación de los escenarios de desastre 7](#_Toc41000779)

[4.3.1. Conectividad interrumpida. 8](#_Toc41000780)

[4.3.2. Mantenimiento con eventos inesperados 8](#_Toc41000781)

[4.4. Centro de datos alterno 9](#_Toc41000782)

[5. PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO 9](#_Toc41000783)

[5.1 Procedimiento de notificación 11](#_Toc41000784)

[5.2 Detección del evento 12](#_Toc41000785)

# INTRODUCCIÓN

La implementación de un proceso de contingencia ante situaciones imprevistas y catastróficas busca minimizar el impacto de la recuperación por perdida de activos de información, a un nivel aceptable implementando una combinación de controles preventivos y de recuperación.

En este proceso se identifican los procesos críticos integrando los requisitos de la gestión de la seguridad de la información para la continuidad de los servicios de (F)EMPOWER.

Las consecuencias de eventos tales como desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio, se someten a un análisis del impacto que busca desarrollar e implementar un plan de continuidad que busque garantizar la restauración oportuna de los servicios.

Este plan de contingencia busca disminuir el impacto de los incidentes imprevistos o catastróficos para los cuales en caso de presentarse estaremos preparados para responder adecuada y oportunamente, reduciendo de manera significativa el impacto a los usuarios de los servicios.

# TERMINOS Y DEFINICIONES

Definición clara y unificada de términos, definiciones y abreviaturas usados en este documento.

**Actividades prioritarias:** Actividades priorizadas después de un incidente con el objetivo de mitigar impactos. Se clasifican como críticas, esenciales, vitales, urgentes y principales.

**Amenaza:** Posibilidad de ocurrencia de un hecho dañino sobre los servicios prestados por (F)EMPOWER, que pueden representar pérdidas de información.

**Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo que busca determinar el nivel de riesgo.

**Continuidad del Servicio:** Capacidad de (F)EMPOWER para continuar con la prestación de los servicios a niveles aceptables luego de un incidente.

**Crisis**: Situación anormal e inestable.

**Desastre:** Evento repentino, inesperado y catastrófico que causa daño o pérdida.

* Evento que pone en peligro la capacidad de la prestación de los servicios por un cierto período de tiempo inaceptable.
* Evento en el que se invoca el plan de contingencia.

**Emergencia**: Evento o incidente que sucede repentinamente y que requiere intervención inmediata para minimizar y controlar la pérdida de información o interrupción de los servicios hasta el punto de que puede representar una amenaza.

**Evento:** Hecho o suceso imprevisto. Ocurrencia o cambio de un conjunto particular de circunstancias.

Puede tener una o más ocurrencias, puede tener varias causas. Puede consistir en algo que no está sucediendo. Puede ser algunas veces referido o conocido como incidente o accidente. Cuando se presenta sin consecuencias puede ser referido como “evento fallido”, “incidente”, “evento cercano”, “evento de aviso”.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar el riesgo.

**Infraestructura:** Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de los servicios prestados.

**Impacto:** Efecto, aceptable o no, de un evento.

**Incidente:** Situación que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe.

**Mitigación:** Medidas a implementar para disminuir o eliminar la ocurrencia o impacto de un evento.

**MTPD (Maximun Tolerable Period of Disruption):** Tiempo máximo permitido para los impactos adversos, como no proveer los servicios.

**Plan de Contingencia:** Documento que contiene un conjunto de acciones y procedimientos definidos, con responsabilidades, para la recuperación del sistema informático que presta los servicios.

**Plan de continuidad:** Procedimientos documentados de guía para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.

**Procesos críticos:** Todos aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

**Proveedor:** Persona, natural o jurídica responsable de suministrar bienes y servicios.

**Respuesta a incidentes:** Acciones realizadas ante un desastre u otro evento importante que pueda afectar significativamente la información y los servicios prestados.

**Recovery Time Objective (RTO):** Tiempo aceptado para que los servicios o la información sean recuperados.

**Recovery Point Objective (RPO):** Punto de restauración en el cual la información debe ser restaurada para permitir la reanudación de los servicios.

# OBJETIVO

Describir las acciones necesarias a ejecutar para la activación del plan de contingencia, para respaldar las aplicaciones en el hosting cloud para asegurar la continuidad de los servicios ante un desastre o contingencia e iniciar con el correcto funcionamiento de los servicios.

# ALCANCE

Como parte de la construcción del presente documento se incluye la información relacionada con las estrategias implementadas para garantizar el respaldo y posterior restauración de la información que permite la recuperación de los servicios.

Servidores:

|  |  |  |  |
| --- | --- | --- | --- |
| **MAQUINA** | **FUNCIÓN O SERVICIO ASOCIADO** | **RPO** | **RTO** |
| a2plcpnl0710 | MySQL Server | 12 Horas | 12 Horas |
| a2plcpnl0710 | Web server | 12 Horas | 12 Horas |
| a2plcpnl0710 | PHP Server | 12 Horas | 12 Horas |
| a2plcpnl0710 | Apache Server | 12 Horas | 12 Horas |

Servicios de conectividad:

|  |  |  |  |
| --- | --- | --- | --- |
| **MAQUINA** | **FUNCIÓN O SERVICIO ASOCIADO** | **RPO** | **RTO** |
| Telecomunicación o transmission digital | El proveedor GoDaddy manifiesta: “…intentar brindar este Sitio y los Servicios durante las veinticuatro (24) horas del día, los siete (7) días de la semana. Usted reconoce y acepta que, de vez en cuando, no se podrá acceder a este Sitio u operarlo por cualquier motivo; incluidas, entre otras, las fallas en los equipos; operaciones de reparación o mantenimiento periódicas que podamos efectuar ocasionalmente; o causas que se encuentren fuera de nuestro control o que no podamos prever de manera razonable, incluidas, entre otras, las interrupciones o fallas en los vínculos de telecomunicación o transmisión digital, ataques hostiles a la red, congestión de la red u otras fallas…” | Dependiendo del evento  Máximo 24H | |

# GENERALIDADES DEL PLAN DE CONTINGENCIA

De acuerdo con la descripción del alcance se definieron tiempos de RTO y RPO para la máquina en servicio.



Operación Normal

Operación en contingencia

**Contingencia**

**RPO**

**RTO**

***Sin servicio***

|  |  |
| --- | --- |
| **Que tan actualizados necesitan estar los datos** | **Cuál es la tolerancia a la no disponibilidad** |

# Estrategia general de recuperación

Este plan considera que por alguna situación crítica interna o externa, no haya acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo o son inaccesibles por completo por un período inaceptable de tiempo.

Las estrategias para seguir serán acordes a la magnitud y duración tentativa 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.

Este plan solo se activará previa aprobación de la dirección.

# Estrategia de acción

Las estrategias y planes de acción consideran la recuperación de información y puesta en funcionamiento de los servicios.

Este plan se desarrolla teniendo en cuenta que la operación de los servicios requiere estar disponible para los usuarios.

**Incidencia Menor:**

En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por el proveedor de hosting o en su defecto dependiendo de la incidencia por el ingeniero de desarrollo o el ingeniero de bases de datos.

**Incidencia Mayor:**

De presentarse una incidencia mayor, se esperará un tiempo prudente que le permita al proveedor del hosting recuperar el servidor. Si el tiempo estimado de reparación que determine GoDaddy, es superior al tiempo identificado para que este operativo, se activará el plan de contingencia.

**Incidencia Catastrófica:**

Si se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa los servicios.

# Clasificación de los escenarios de desastre

En esta sección se incluye una clasificación de los posibles escenarios de desastre que pueden Ocurrir.

**Clasificación escenarios de desastre**

# Conectividad interrumpida.

Por razones desconocidas no es posible acceder al servidor remoto, caída de internet.

# Mantenimiento con eventos inesperados

* + - * Daños inesperados causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones de mantenimiento dando cumplimiento a sus obligaciones.
      * Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética que alteren y/o interrumpan el normal funcionamiento del servidor.
      * Por problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, corrupción de la base de datos 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.
      * Pérdida del hardware, software e información.
      * 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.

# Centro de datos alterno

En la actualidad no se cuenta con sitio de datos alternos, sin embargo, los respaldos realizados a la información son almacenados fuera del servidor, y en una ubicación geográfica diferente.

# PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO

Se realizará notificación de la situación a los usuarios y a los interesados que se consideren pertinentes informando la situación y las estrategias implementadas para superar la situación, dando un tiempo estimado para la resolución.

A continuación, se listan las actividades a ejecutar cuando se active la contingencia, de acuerdo con la presentación de cualquier tipo de evento adverso:

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de evento** | **Características** | **Ejemplos** | **Respuesta** |
| **DESASTRE** | Inhabilita el Hosting. No permite acceder ni utilizar los servicios. | Terremotos, incendio general, fallo eléctrico en el sector. | Plan de contingencia |
| **INTERRUPCIÓN** | Evento que se evalúa para determinar si es tratado como desastre o como contingencia. | Incendio localizado, atentado terrorista, huelga interno o externo. | Planes de contingencia |
| **CONTINGENCIA** | Un servicio se afecta. No impide el acceso al portal, pero si a algunos servicios. Requiere evaluación que puede llevarla a categoría de desastre. | Fallo de sistemas o servicio, ausencia de personal clave. | Planes de contingencia |

**Clasificación de eventos**

**Fases de activación**

Actividades adicionales a las fases definidas anteriormente:

* 1. Registro de Incidente
  2. Evaluación inicial
  3. Definición de la criticidad
  4. Comunicaciones.
  5. Generación de alertas
  6. Activar Desastre
  7. Activación del plan de contingencia
  8. Ejecución Plan de contingencia
  9. Notificación Contingencia
  10. Monitoreo y Seguimiento periodo de contingencia
  11. Comunicación continúa interna/externa con involucrados
  12. Declaración de fin de contingencia
  13. Regreso a modo normal de operación
  14. Notificación formal de fin de contingencia
  15. Actualización del plan de contingencia
  16. Documentación de lecciones aprendidas
  17. Actualización Planes de Prueba
  18. Fin de Contingencia

# Procedimiento de notificación

Cuando se presenta una emergencia, hay que tener en cuenta que se debe gestionar la notificación de la misma con el ánimo de iniciar con el proceso de activación del Plan de Recuperación de Desastres (DRP). Esta notificación corresponde a una gestión para la activación del plan la cual se describe a continuación:

**Procedimiento de notificación**

La notificación de la indisponibilidad de los sistemas de información o servicios de TI puede llegar por diferentes fuentes, esto dependerá de la naturaleza del evento, del momento en el cual éste suceda y de la fuente que lo causa.

Proceso mediante el cual se activa la gestión del plan, previa notificación del desastre, y hasta el momento en que el servicio es restaurado:

**Proceso de activación gestión del plan**

El procedimiento de entrada a contingencia describe las actividades requeridas para la activación de los diferentes servicios que se encuentran respaldados en el centro de datos, cuando se activa el plan.

# Detección del evento

Los eventos que afectan la continuidad de las operaciones de los servicios y maquinas se reportan en cuanto se identifican con el fin de iniciar a trabajar en una pronta atención y por ende el cumplimiento de los tiempos de atención, los RTO’s y RPO´s definidos.

La detección se realizará una vez se presenten interrupciones de los servicios:

* + 1. Portal institucional.
    2. Aplicación web.

Los anteriores servicios descritos, fueron definidos como críticos, y en ellos se relacionan la totalidad de las maquinas que se encuentran en el alcance para su correcto funcionamiento.

A continuación, se relacionan algunos medios de comunicación a ser utilizados al momento de un evento adverso, así como su prioridad en usabilidad:

|  |  |  |
| --- | --- | --- |
| **MEDIOS DE COMUNICACIÓN** | | |
| **Prioridad** | **Tipos de Medio** | **Descripción** |
| 1 | Persona a Persona | La forma más fácil y efectiva. Debe ser explícito y detallar lo sucedido con el evento. La comunicación depende de factores socio-ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación. |
| 2 | Telefonía Celular | La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con él se puede al igual que en la comunicación persona a persona ser más explícito y ahondar dentro de la comunicación del evento. |
| 3 | Telefonía Fija |
| 4 | Skype - Viber  (requiere Smartphone e internet) |
| 5 | Mensajería Instantánea – Link (requiere Computador Personal e internet Whats Up (requiere Smartphone e  internet) | La mensajería instantánea como un tipo de correo permite interactuar más rápida y efectivamente entre una o varias personas. Depende de los medios, las restricciones y de la disposición de los intercomunicadores. |
| 6 | Correo Electrónico | El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo. Este tipo de comunicación depende del grado  de consulta de los intercomunicadores. |
| 7 | Correo Físico Certificado | El correo certificado permite enviar documentos de forma más segura a cualquier destinatario. |
| 8 | Correo Físico Normal | El correo físico normal, es uno de los medios más antiguos y que sigue teniendo vigencia. |
| 9 | Redes sociales (Facebook, Twitter y Google +) | Para ubicar a las personas. |

**Medios de comunicación**

**HISTORIAL DE CAMBIOS**

|  |  |  |
| --- | --- | --- |
| **VERSION** | **FECHA** | **DESCRIPCION** |
| 00 | 01/04/2020 | Creación del documento. |
| 01 | 18/05/2020 | Actualización del documento. |

|  |  |  |
| --- | --- | --- |
| **Elaboró** | **Revisó** | **Aprobó** |
| **A close up of a logo  Description automatically generated** | **A close up of a logo  Description automatically generated** | **A close up of a logo  Description automatically generated** |
| **Marcela Inés Sánchez** | **Natalia Gamboa** | **Natalia Gamboa** |