MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES

Empresa De Servicios Públicos De Chía Emserchia E.S.P.

Área de Sistemas de información

Contenido

1. INTRODUCCIÓN 3
2. TERMINOS Y DEFINICIONES 3
3. OBJETIVO 6
4. ALCANCE 7
5. GENERALIDADES DEL PLAN DE RECUPERACION DE DESASTRES (RDP) 7
6. ESTRATEGIA GENERAL DE RECUPERACION. 8
6.1 ESTRATEGIAS DE ACCION 8
6.2 INCIDENCIA MENOR 8
6.3 INCIDENCIA MAYOR 8
6.4 INCIDENCIA CATASTROFICA 9
6.5 PERDIDA TOTAL O PARCIAL DE LAS INSTALACIONES DEL CENTRO DE DATOS 9
6.6 PERDIDA TOTAL O PARCIAL DE LOS SERVICIOS PACTADOR EN EL DRP 9
7 MARCO LEGAL 10
8 PROCEDIMIENTOS DE NOTIFICACION, ACTIVACION Y RETORNO 10
8.1 PROCEDIMIENTO DE NOTIFICACION 9
8.2 DETECCION DEL EVENTO 10
8.3 DEFINICION DE RECURSOS 10
8.4 COMITÉ DE EMERGENCIAS 10
8.5 COMITÉ RESPONSABLE DE LA ACTIVACION DEL DRP 10
8.6 EQUIPO DE RECUPERACION DEL DRP 10
9 ARBOL DE LLAMADAS. 15

INTRODUCCIÓN

La Empresa de servicios Públicos de Chía Emserchia E.S.P., dando cumplimiento al decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* y reconociendo la necesidad de proteger los activos de información de la entidad mediante un modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información.

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.
Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deberían ser someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

La correcta implementación de la gestión de la continuidad del negocio disminuirá el impacto al presentarse incidentes disruptivos y en caso de producirse, la entidad estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

1. TERMINOS Y DEFINICIONES

El ítem de términos y definiciones se elabora para lograr entendimiento de forma clara y unificación de la terminología, definiciones y abreviaturas que tengan lugar en el presente documento.

ACTIVIDADES PRIORITARIAS: Actividades a las que se les debe dar prioridad después de un incidente a fin de mitigar los impactos. Nota: Los términos que comúnmente se utilizan para describir las actividades dentro de este grupo son: critico, esencial, vital, urgente y principal. Dentro del desarrollo de este documento se utiliza el término actividades críticas. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.42].

AMENAZA: Percepción de la posibilidad de ocurrencia de algún hecho dañino sobre los recursos involucrados en el desarrollo de un proceso (humano, financiero, medio ambiente, información e imagen corporativa), representando pérdidas para el sistema o la organización. (International Glossary of Reslience).

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. Nota 1: El análisis de riesgo proporciona las bases para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. Nota 2: El análisis del riesgo incluye la estimación del riesgo. [Norma ISO 31000:2011, Capitulo 2, Términos y definiciones, numeral 2.21].

CENTRO ALTERNO DE PROCESAMIENTO DE DATOS (CAPD): Lugar en donde se procesa la información de una entidad cuando no es posible hacerlo en el CPD, independientemente de ser de su propiedad o de un tercero. Centro de Procesamiento de Datos (CPD): Lugar en donde se concentran los recursos necesarios para el procesamiento de la información de una entidad, independientemente de ser de su propiedad o de un tercero.

CONTINUIDAD DEL NEGOCIO: Capacidad de la organización para continuar con la entrega de sus productos o servicios a niveles aceptables predefinidos luego de un incidente disruptivo. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.3]

CRISIS: Situación anormal e inestable que amenaza los objetivos estratégicos, la reputación o la viabilidad de una organización. [BS 11200:2014 – Crisis Management – Guiadance and good practice, Capitulo 2, Términos y definiciones]

DESASTRE: Un evento repentino, no planeado y catastrófico que causa daño o pérdida no aceptable a una organización.
Un evento que pone en peligro la capacidad de una organización para proporcionar funciones críticas, procesos o servicios por un cierto período de tiempo inaceptable.

Un evento en el que la gestión de una organización invoca sus planes de recuperación. [Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

DIRECTORIO ACTIVO: Base de datos distribuida que permite almacenar información relativa a los recursos de una red (objetos, dominios, árboles y bosques) con el fin de facilitar su localización y administración, el cual ofrece la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa.

EJERCICIO: Proceso para entrenarse, prepararse, practicar y mejorar el desempeño de una organización. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.18]

EMERGENCIA: Un evento o incidente imprevisto que sucede repentinamente y demanda acción e intervención inmediata para minimizar pérdidas potenciales de vidas, destrucción de propiedades o la pérdida o interrupción de las operaciones de negocio hasta el punto que pueda representar una amenaza. [Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

EVENTO: Hecho o suceso imprevisto. Es la ocurrencia o cambio de un conjunto particular de circunstancias. Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas. Nota 2: Un evento puede consistir en algo que no está sucediendo. Nota 3: Un evento puede ser algunas veces referido o conocido como incidente o accidente. Nota 4: Un evento sin consecuencias

puede ser referido como "evento fallido", "incidente", "evento cercano", "evento de aviso" [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.17].

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.51].

INFRAESTRUCTURA: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.20].

IMPACTO: Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector.
[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

INCIDENTE: Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe.
[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency

MITIGACIÓN: Implementación de medidas para disminuir o eliminar la ocurrencia o impacto de un evento.
[Disaster Recovery Institute International - DRI International –Glossary for Resiliency

MTPD (Maximun Tolerable Period of Disruption): Tiempo para que los impactos adversos, los cuales pueden surgir del resultado de no proveer un producto o servicio o realizar una actividad, sea inaceptable.
[Norma ISO 22301:2012, Capitulo 3, Términos y definiciones; numeral 3.26]

PLAN DE RECUPERACIÓN ANTE DESASTRES (Disaster Recovery Plan – DRP): Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.
[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

PLAN DE CONTINUIDAD DEL NEGOCIO (PCN): Conjunto de procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.
[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - "Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos", capitulo 2, numeral 2.6]

PROCESOS CRÍTICOS: Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.
[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - "Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos", capitulo 2, numeral 2.7.1]

RESPUESTA A INCIDENTES: Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable.
[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

RECOVERY TIME OBJECTIVE (RTO): Tiempo después de un incidente en el que la operación o el servicio deben ser reanudados.
[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia -Capítulo XXIX - CE 026 del 2016 - "Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos", capitulo 2, numeral 2.9]

RECOVERY POINT OBJECTIVE (RPO): Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.
[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia -Capítulo XXIX - CE 026 del 2016 - "Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos", capitulo 2, numeral 2.8]

BUSINESS IMPACT ANALYSIS (BIA): es una etapa que permite identificar la urgencia de recuperación de cada procedimiento, los recursos y sistemas críticos para estimar el tiempo que puede tolerar en caso de un incidente o desastre.

2. OBJETIVO

Describir las acciones necesarias a ejecutar para la activación del plan de recuperación desastres DRP en el centro de datos de EMSERCHIA E.S.P. para respaldar las aplicaciones críticas con el fin

de asegurar la continuidad de la operación ante un desastre o contingencia e iniciar con el correcto funcionamiento de los servicios identificados como críticos de EMSERCHIA E.S.P

3. ALCANCE

La necesidad de desarrollar un plan de contingencia está relacionado con el impacto potencial que provoca la interrupción parcial o total de los servicios y los aplicativos críticos de EMSERCHIA E.S.P, sobre el normal desarrollo de las actividades, específicamente, para afrontar la contingencia relacionada con el eventual cese de las actividades e inoperatividad de los servicios, buscando mantener funcionando los sistemas críticos y los servicios que la entidad ofrece como sysman, corrycom plataforma de correos , dominio y aplicaciones de EMSERCHIA E.S.P. Y los procesos a seguir durante las pruebas y en caso de un evento adverso en que se requiera la activación del plan.

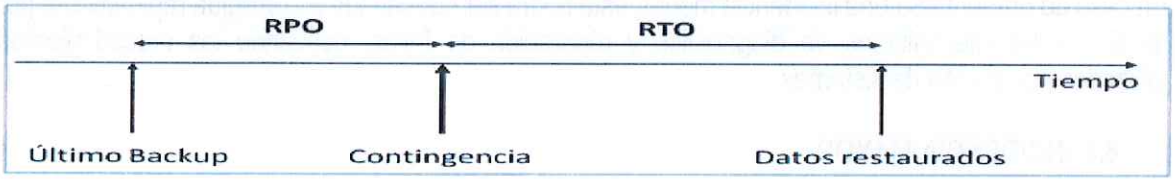
Servidores que hacen parte del DRP:

EQUIPO	FUNCION O SERVICIO ASOCIADO	RPO	RTO
SYSMAN	Servidor ERP	4 Horas	4 Horas
CORRYCOM	Servidor gestión documental	3 Horas	3 Horas
APLICACIONES	Servidor de aplicaciones	3 Horas	3 Horas
DOMINIO	Servidor de Dominio-File Server	3 Horas	3 Horas

El cumplimiento del RPO y RTO se verificara en las pruebas realizadas ocasionalmente en el servidor alterno .(ubicado en CAU Curubito)

4. GENERALIDADES DEL PLAN DE RECUPERACION DE DESASTRES (RDP)

De acuerdo con la descripción del alcance el área de sistemas de EMSERCHIA E.S.P. Definió unos tiempos de RTO y RPO para cada uno de los servicios alojados en los servidores.



5. ESTRATEGIA GENERAL DE RECUPERACION.

Este plan está basado en el hecho de que por alguna situación crítica interna o externa, no haya acceso a los servicios que se encuentran centralizados en nuestro centro de datos o son inaccesibles por completo o por un periodo de tiempo.
Las estrategias a seguir serán acordes a la magnitud y duración del incidente y se deberán tener en cuenta los siguientes aspectos:

- Evaluación de los daños
- Evaluación del tiempo estimado de la recuperación.
- Análisis para determinar las acciones específicas que deben seguirse de acuerdo al tipo de incidente.

El área de sistemas de EMSERCHIA E.S.P. Determino contar con un servidor alterno para respaldo de copias de seguridad ubicado en otro lugar geográfico, fuera de la oficina principal.

6.1 ESTRATEGIAS DE ACCION

Las estrategias y planes de acción han sido orientados a cubrir una contingencia que inhabilite al acceso a los servicios de cómputo y telecomunicaciones en que se apoyan todas las aplicaciones críticas de EMSERCHIA E.S.P. como:

- Servidor SYSMAN
- Servidor CORRYCOM
- Servidor APLICACIONES
- Servidor de DOMINIO.

La decisión para desarrollar este plan, se basó en las características actuales de EMSERCHIA E.S.P. así como el nivel de dependencia de tecnología de información y comunicaciones.

6.2 INCIDENCIA MENOR

En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de diagnóstico y reparación de fallas, activando los procedimientos utilizados por el área de sistemas.

6.3 INCIDENCIA MAYOR

De presentarse una incidencia mayor en los equipos y sistemas del centro de datos que impidan la función general de la empresa, esta deberá ser identificada y corregida en el menor tiempo posible. Si el tiempo estimado de reparación que se determine por el área de sistemas es superior al tiempo identificado para que este operativo el área de sistemas de EMSERCHIA E.S.P. tomara la decisión de activar o no el DRP.

6.4 INCIDENCIA CATASTROFICA

Si se presenta un incidente mayor en los equipos y sistemas del centro de datos principal que impida la función general de EMSERCHIA E.S.P. Esta deberá ser identificada y corregida a la brevedad. Si

el tiempo estimado de reparación que determinen los equipos de recuperación responsables de los aplicativos o recursos técnicos es superior al tiempo identificado para que este operativo, EMSERCHIA E.S.P tomara la decisión de activar o no el plan DRP.

6.5 PERDIDA TOTAL O PARCIAL DE LAS INSTALACIONES DEL CENTRO DE DATOS

La pérdida total o parcial de las instalaciones del centro de datos de EMSERCHIA E.S.P puede deberse a diferentes situaciones como:

- ✓ Actos perpetuados por terroristas o grupos armados ilegales.
- ✓ Asonada o conmoción popular.
- ✓ Temblores, terremotos, inundaciones, o cualquier otra convulsión de la naturaleza.
- ✓ Radiaciones o contaminación radioactiva.

6.6 PERDIDA TOTAL O PARCIAL DE LOS SERVICIOS PACTADOR EN EL DRP

La pérdida total o parcial de los servicios puede originarse por las siguientes razones:

- ✓ Daños causados por las personas de TI en el curso de ejecución de las operaciones con el propósito de dar cumplimiento a sus obligaciones.
- ✓ Por la omisión de procedimientos establecidos para la prestación de los servicios de TI.
- ✓ Por delitos informáticos, y utilización de técnicas como acceso a los activos de la información por medio de identidad falsa o algún tipo de ingeniería social.
- ✓ Por vulnerabilidades en sistemas operativos y aplicaciones alojadas en el centro de datos.
- ✓ Por inyección de códigos maliciosos tales como puertas traseras, ataques de denegación de servicios, virus que puedan generar la pérdida total o parcial de los datos.
- ✓ Por exposición de acceso físico tales como entradas no autorizadas a nuestro centro de datos con el fin de hacer algún daño, vandalismo o alteración de equipos e información sensible.
- ✓ Problemas por fallas eléctricas que interrumpan el normal funcionamiento de los equipos.
- ✓ Daño total o parcial del hardware debido a deterioros causados por calor o desgaste de algún elemento electrónico.

7 MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 1008 de 2018 ""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Artículo 61 de la Constitución Política de Colombia.
- Decisión Andina 351 de 1993. - Derechos de Autor
- Código Civil, Artículo 671. - PROPIEDAD INTELECTUAL. Las producciones del talento o del ingenio son una propiedad de sus autores.
- Ley 23 de 1982. – Derechos de Autor
- Ley 44 de 1993. – Derechos de Autor

8 PROCEDIMIENTOS DE NOTIFICACION, ACTIVACION Y RETORNO

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan unas tareas que deben realizarse lo más pronto posible, después de presentarse el incidente.

Estas son las actividades a ejecutar cuando se active la contingencia:

TIPO DE EVENTO	CARACTERISTICAS	EJEMPLOS	RESPUESTA
DESASTRE	Este evento inhabilita el datacenter y no permite seguir prestando los servicios.	Terremoto, incendio, fallo eléctrico.	DRP
INTERRUPCION	Este evento requiere evaluación y ser tratado como contingencia dependiendo del impacto que se determine.	Incendio localizado, atentado, huelga	DRP Plan de contingencia

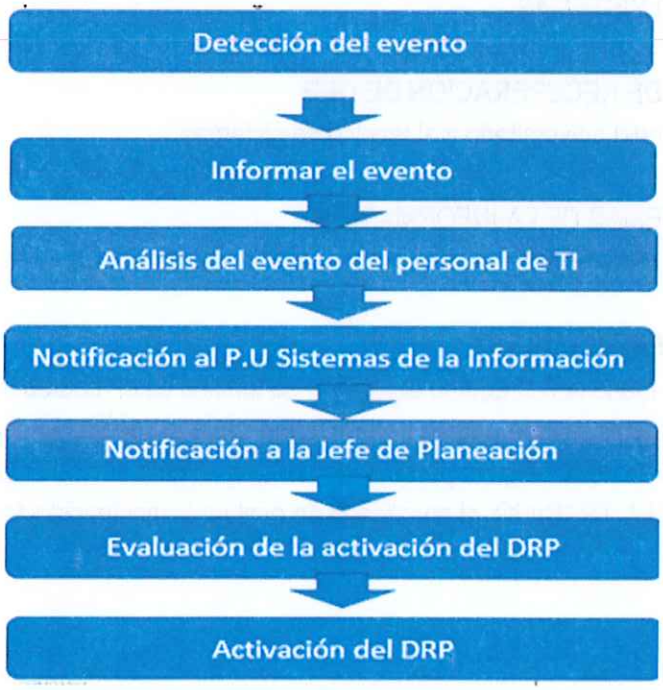
CONTINGENCIA	Este evento afecta puntualmente un recurso para la prestación de un servicio informático, pero no impide seguir prestando los demás servicios	Fallo en un servidor, o algún otro equipo del datacenter	Planes de contingencia

ACTIVIDADES ANEXAS AL PROCEDIMIENTO DE NOTIFICACION, ACTIVACION Y RETORNO.

- ✓ Registro de incidentes
- ✓ Activación del plan de recuperación de desastres
- ✓ Ejecución procedimiento de contingencia
- ✓ Notificación contingencia
- ✓ Monitoreo y seguimiento de la contingencia
- ✓ Activación del plan de retorno de contingencia
- ✓ Notificación de fin de contingencia
- ✓ Regreso a modo normal de operación
- ✓ Notificación formal a Gerencia de fin de contingencia.
- ✓ Actualización laboratorios de prueba
- ✓ Fin de contingencia

8.1 PROCEDIMIENTO DE NOTIFICACION

Cuando se llegue a presentar una emergencia se hará la notificación con el objeto de activar el DRP así:



8.2 DETECCION DEL EVENTO

Los eventos que afecten la continuidad de las operaciones de EMSERCHIA E.S.P podrán ser reportadas una vez se identifique con el fin de iniciar los trabajos para una pronta atención con el fin de cumplir los tiempo de RTO y RPO definidos.

Este reporte de eventos se realizará una vez se presente alguna de las siguientes interrupciones:

- ✓ Fallo o caída del servicio en servidor de SYSMAN
- ✓ Fallo o caída del servicio en servidor de CORRYCOM
- ✓ Fallo o caída del servicio en servidor de APLICACIONES
- ✓ Fallo o caída del servicio en servidor de DOMINIO
- ✓ Fallo en dominio de correos
- ✓ Fallo en página WEB de EMSERCHIA E.S.P
- ✓ Fallo de internet
- ✓ Fallo de firewall o switch capa 3
- ✓ Fallo eléctrico.

8.3 DEFINICION DE RECURSOS

Como parte del DRP se asignan los miembros que atenderán las solicitudes asi:

- ✓ **RESPONSABLE DE LA ACTIVACION DEL DRP**
  P.U SISTEMAS DE LA INFORMACION
  TECNICO SISTEMAS

- ✓ **EQUIPO DE RECUPERACION DE DRP**
  El profesional universitario y el técnico de sistemas.

  P.U SISTEMAS DE LA INFORMACION
  TECNICO SISTEMAS

8.4 COMITÉ DE EMERGENCIAS.

Trabaja de la mano con el equipo del DRP y su función es el recurso humano o salvaguardar las vidas humanas, a este equipo se le informa de la incidencia si dado el caso se ha visto involucrada o en riesgo alguna persona de nuestra entidad siendo el equipo de SEGURIDAD Y SALUD EN EL TRABAJO el encargado de evaluar la incidencia y la toma de decisiones.

8.5 COMITÉ RESPONSABLE DE LA ACTIVACION DEL DRP.

Está conformado por el Profesional Universitario de Sistemas de la Información y el Técnico de Sistemas que son las personas de TI de EMSERCHIA E.S.P

Se debe asegurar la comunicación permanente con Gerencia y directores de EMSERCHIA E.S.P. antes y después de la incidencia.

8.6 EQUIPO DE RECUPERACION DEL DRP.

Está compuesto por el equipo responsable de la Oficina de Sistemas, se encarga de restablecer la operación de los servicios de hardware, software, telecomunicaciones, energía que dificulten la continuación de la operación.

FUNCIONES PRINCIPALES.

- ✓ Llevar a cabo los procedimientos de recuperación de la operación cuando se declare la contingencia.
- ✓ Mantener un inventario y registro actualizado de los equipos y aplicaciones y demás componentes que integran la infraestructura Tecnológica de EMSERCHIA E.S.P.
- ✓ Mantener actualizadas las copias de respaldo en caso de algún evento o contingencia.
- ✓ Identificar debilidades de la Infraestructura Tecnológica.
- ✓ Mantener actualizados los contactos de proveedores Tecnológicos en caso de una contingencia.
- ✓ Evaluar el tipo de daño ocurrido sobre el o los servicios reportados.
- ✓ Informar a Gerencia sobre el avance y el tiempo de recuperación estimados.
- ✓ Ejecutar las acciones de DRP.

Dentro del equipo de recuperación se encuentran los diferentes sistemas y las responsabilidades son las siguientes:

EQUIPOS PLATAFORMA WINDOWS.

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios de los servidores de la plataforma Windows sobre los cuales funcionan: ERP SYSMAN, SERVIDOR DE APLICACIONES, SERVIDOR DE DOMINIO, SERVIDOR DE CORRYCOM. Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad de las actualizaciones, respaldo y nos permitan el restablecimiento de los servicios.

Algunas de las responsabilidades de este equipo son:

- ✓ Mantener actualizados los servidores tanto en hardware como en software.

- ✓ Conocer y divulgar con el equipo de TI los procedimientos en caso de desastre.
- ✓ Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- ✓ Ejecutar pruebas del DRP en lo referente a esta plataforma.
- ✓ Determinar el impacto en caso de falla y emitir concepto para la toma de decisiones.
- ✓ Asistir la recuperación de la plataforma.
- ✓ Documentar fallas y soluciones.
- ✓ Restablecer los servicios de esta plataforma en el Centro de Datos.

EQUIPO DE BASE DE DATOS.

- ✓ Mantener actualizado el servidor y NAS de las bases de datos
- ✓ Conocer y divulgar con el equipo de TI los procedimientos en caso de desastre.
- ✓ Verificar la realización de las copias de seguridad
- ✓ Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- ✓ Ejecutar pruebas de DRP instalando una base de datos de prueba y revisando que funcione normalmente
- ✓ Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- ✓ Ejecutar las pruebas de DRP en lo referente a esta plataforma.
- ✓ Restaurar los servicios en el Centro de Cómputo.

EQUIPOS DE CONECTIVIDAD.

Es el responsable de planear y coordinar las actividades que permitan la activación de los servicios específicos de conectividad sobre los cuales se apoya la entrega de los servicios de TI.

Algunas de las responsabilidades de este equipo son:

- ✓ Mantener actualizadas las configuraciones de los equipos FW, SW. AP.
- ✓ Ejecutar pruebas de DRP en estos equipos.
- ✓ Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- ✓ Documentar las fallas y las soluciones.
- ✓ Reactivar los servicios.

EQUIPO DE USUARIOS.

Corresponde al grupo de personas responsables del equipo de TI de EMSERCHIA E.S.P. en la administración de las aplicaciones.

Algunas de las responsabilidades de este equipo son:

- ✓ Información y notificación de eventos identificados a nivel de sus procesos que puedan afectar las operaciones.

- ✓ Apoyar al interior de su proceso los aspectos de continuidad, indicando acciones de mejora.
- ✓ El equipo de soporte debe brindar el soporte a los usuarios finales de EMSERCHIA E.S.P para el normal desarrollo de sus actividades.

El equipo está conformado por:

- ✓ P.U SISTEMAS DE LA INFORMACION
- ✓ TECNICO DE SISTEMAS.

RESPONSABILIDADES.

- ✓ Conocer y entender el Plan de Contingencia.
- ✓ Verificar con los usuarios finales de EMSERCHIA E.S.P la estabilidad de las aplicaciones.
- ✓ Cooperar con el equipo de Recuperación de Contingencias en la puesta en marcha.

RESPONSABLES DE LA OFICINA DE TI PARA LA ACTIVACION DEL DRP.

ING.HUMBERTO BARAJAS LOPEZ
P.U SISTEMAS DE LA INFORMACION.
sistemas@emserchia.gov.co
cel.3206389585

OSMITH HERNANDEZ CRESPO
TECNICO SISTEMAS
tecnicosistemas@emserchia.gov.co

9 ARBOL DE LLAMADAS.

El árbol de llamadas representa la cadena de llamadas que se debe seguir y cumplir para comunicarse con los integrantes del DRP la activación del plan, esta se ejecuta después de la declaración realizada por el P.U SISTEMAS DE LA INFORMACION.

A continuación se relacionan algunos medios de comunicación ser utilizados al momento de un evento adverso:

PRIORIDAD	TIPOS DE MEDIO	DESCRIPCION
1	Perona a Persona	La forma más fácil y efectiva de comunicar el evento es hacerlo persona a persona. Este medio permite ser más explícito y detallar lo sucedido con el evento.
2	Telefonía Celular	La comunicación por los equipos celulares para comunicar el evento
3	Telefonía fija	Comunicación al número de la extensión fija del área de TI
4	Correo Electrónico	El correo electrónico es un medio efectivo quedando el registro de la solicitud del evento.

ELABORO : HUMBERTO BARAJAS LOPEZ
P.U SISTEMAS DE LA INFORMACION.

REVISO: ANDRES JULIAN FENDEZ CASTRO
SUBGERENTE ESTRATÉGICO