	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-G0-05
		Versión	01
		Fecha	03-12-2018

TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES

MANUAL DE INFORMATICA DE POLITICAS DE SEGURIDAD DE LA EMRU EIC.

Versión 01

Área de Informática

Diciembre de 2018



**MANUAL DE PLAN DE CONTINGENCIA  
INFORMATICA**

Código	PR-GO-25
Versión	01
Fecha	03-12-2018

**TABLA DE CONTENIDO**

1. INTRODUCCIÓN.....	2
2. GENERALIDADES.....	3
2.1 DEFINICIONES.....	3
3. OBJETIVO GENERAL.....	4
4. OBJETIVOS ESPECÍFICOS.....	5
5. ALCANCE Y RESPONSABILIDADES.....	6
6. TIEMPO DE INACTIVIDAD.....	7
7. PLATAFORMA DE TIC.....	8
7.1 Computador de Escritorio y Portátiles:.....	8
7.2 Impresora y Fotocopiadora.....	8
7.3 Elementos activos de la red de datos.....	8
7.4 Pagina WEB.....	9
7.5 Proveedor de Internet.....	9
8. DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS.....	10
9. ANALISIS DE RIESGOS.....	11
10. EVALUACIÓN Y CALIFICACIÓN DEL IMPACTO DE LOS PROCESOS CRÍTICOS PARA LA CONTINUIDAD DEL SERVICIO.....	13
11. IDENTIFICACIÓN DE RIESGOS Y DEFINICIÓN DE PLANES DE CONTINGENCIA.....	14
11.1 PCs.....	14
11.2 Fotocopiadora.....	14
11.3 Proveedor de Internet EMCALI.....	15
11.4 Pagina Web.....	15
12. CENTRO DE SOPORTE.....	16
13. CONCLUSIONES.....	17

	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 1. INTRODUCCIÓN

El plan de contingencia de tecnologías de información de la EMRU EIC, es un documento que establece los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, daños en equipos de cómputo, equipos de informática o desastres producto de eventos naturales u otros, a causa de algún incidente tanto interno como externo a tecnologías de información.

Durante el desarrollo del presente manual de plan de contingencia, se presentan las actividades propias de gestión de contingencia que debe considerar LA EMRU EIC, cubriendo así los incidentes que afecten el sistema de información. Así mismos aspectos conceptuales que permitan un mayor panorama acerca del entendimiento de las contingencias y que servirán como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencia.

Las causas para aplicar el manual de plan de contingencia pueden ser variadas, como, por ejemplo: daño en los equipos de cómputo de los usuarios finales, daño de impresoras, daño de equipos activos de la red de datos, la elaboración del plan de contingencia implica un importante avance a la hora de superar situaciones de interrupción de las actividades y servicios prestados por la EMRU EIC.

Es indispensable para el éxito del plan de contingencia, contar con personal capacitado y comprometido con la EMRU EIC. dx


	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 2. GENERALIDADES

### 2.1 DEFINICIONES

**PLAN DE CONTINGENCIA:** Entendemos por plan de contingencia el conjunto de procedimientos alternativos a la operativa normal de cada empresa, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la entidad.

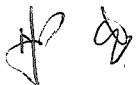
**PLAN DE CONTINGENCIA INFORMATICO:** Es una estrategia planificada, con una serie de procedimientos que nos facilitan y nos orientan, a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización, ante eventos que puedan presentarse en los servicios ya sea de forma parcial o total.


	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

### 3. OBJETIVO GENERAL

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información, para la EMRU EIC.


Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.



	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

#### 4. OBJETIVOS ESPECÍFICOS

- Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de la EMRU EIC.
- Proteger la propiedad de la EMRU EIC.
- Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.
- Continuar con las funciones de las diferentes áreas de la EMRU EIC, que se haya visto afectadas por una situación adversa.
- Prevenir o minimizar el daño permanente a los recursos informáticos.

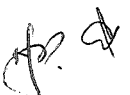
	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 5. ALCANCE Y RESPONSABILIDADES

El plan de contingencia que se desarrolla en el presente documento es de aplicación a todas las áreas funcionales en la estructura orgánico -funcional de la EMRU EIC que hacen uso de los recursos informáticos de la Institución.

El coordinador y/o técnico de sistemas o quien haga sus veces es el responsable de la ejecución del plan de contingencia con el apoyo del equipo de trabajo de la oficina de sistemas o control interno de la entidad.

La copia de los datos almacenados en las estaciones de trabajo o pcs, son responsabilidad de cada uno de los usuarios.




	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 6. TIEMPO DE INACTIVIDAD

Los casos de tiempos de inactividad planeadas pueden ser por cambio del sistema, cambios de datos, reconfiguración del sistemas o reinicio de servicios.

Los casos de tiempos de inactividad no planeadas pueden ser provocados por fallas del sistema, fallas de la red de datos, fallas en el fluido eléctrico o caídas del servicio de internet



	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 7. PLATAFORMA DE TIC

Para una adecuada respuesta ante cualquier eventualidad o falla ocurrida a cualquier recurso informático físico de la EMRU EIC, se cuenta con inventario completo de todos los elementos, el mismo está compuesto así:

### 7.1 Computador de Escritorio y Portátiles:

Se cuentan con equipos de cómputo de marca HP de varias referencias y 1 (un) equipo portátil ASUS X541UJ

### 7.2 Impresora y Fotocopiadora

Se cuentan con impresoras láser jet HP 1006 AF0280 de mediano rendimiento y con una impresora de inyección de tinta EPSON L555.

La fotocopiadora se trabaja bajo un contrato de arrendamiento con la empresa ABKA.

### 7.3 Elementos activos de la red de datos


Toda la red de datos se encuentra bajo dos (2) Router,

1. ROUTER LINKSYS E900 S/N 12312C65608292 y
2. ROUTER LINKSYS E2500 S/N 10A30C64607981

Se cuentan con 1 centro de cableado estructurado con:

- 1 SWITCH 24 PUERTOS 3COM 2024 S/N AC/9N3QAA0107884
- 1 SWITCH 16 PUERTOS 3 COM OFFICECONNECT S/N AB/9E8C810017455
- 1 SWITCH 8 PUERTOS 3 COM OFFICECONNECT
- 1 SWITCH 8 PUERTOS DLINK DES-1008D S/N PL272A5002357



	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

#### **7.4 Pagina WEB**

Alojamiento en Colombia Hosting

#### **7.5 Proveedor de Internet**

Fibra óptica de EMCALI

	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 8. DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS

RECURSO	POSIBILIDAD DE DAÑO	PERIODO PARA SOLUCION
PC	MEDIA/AL TA	4 HORAS
PROVEEDOR DE INTERNET	BAJA	2 horas
IMPRESORA	MEDIA/AL TA	INMEDIATA
FOTOCOPIADORA	BAJA	8 horas hábiles
RED INALÁMBRICA	BAJA	Inmediata
FLUJO ELECTRICO	BAJA	1 DIA

	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 9. ANALISIS DE RIESGOS

Para realizar un análisis de los riesgos, se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la EMRU EIC, y su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

### **Bienes susceptibles de un daño**

Se puede identificar los siguientes bienes afectos a riesgos:

- a) Personal
- b) Hardware
- c) Software y utilitarios
- d) Datos e información
- e) Documentación
- f) Suministro de energía eléctrica
- g) Suministro de telecomunicaciones

### **Daños**


Los posibles daños pueden referirse a:

- a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese, por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado. Divulgación de información a instancias fuera de la EMRU EIC y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

### **Prioridades**

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios



	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	
	Código	PR-GO-25
	Versión	01
	Fecha	03-12-2018

que se pierden en el acontecimiento. Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre. ( La Información activo mas importante)

### **Fuentes de daño**

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía asociadas a la EMRU EIC son:

Acceso no autorizado

Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones) de las claves de acceso a los sistemas computacionales)

Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje). b) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

### **Desastres Naturales**

- a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).
- b) Inundaciones causados por falla en los suministros de agua.

### **Otras Fallas**

Fallas en los equipos de soporte:

- a) Por fallas causadas por la agresividad del ambiente
- b) Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por parte de la entidad.

Por fallas de la comunicación.

- a) Por fallas en el tendido físico de la red local.
- b) Fallas en las telecomunicaciones con instalaciones externas.
- c) Por fallas de Conmutador Líneas telefónicas del PBX.

Fallas de Hardware

- a) Falla en el PCs en aplicaciones y datos, tanto en su disco duro como los respaldos
- b) Falla en el hardware de Red:
- c) Falla en los Switches.
- d) Falla en el cableado de la Red.
- e) Falla en el Router.
- f) Falla en el FireWall.
- g) Caída del servicio de Internet



	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 10. EVALUACIÓN Y CALIFICACIÓN DEL IMPACTO DE LOS PROCESOS CRÍTICOS PARA LA CONTINUIDAD DEL SERVICIO

RECURSOS	NIVEL DE IMPACTO
Estaciones de trabajo PCs	2
Sistema de Información	3
Página WEB	2
Proveedor internet EMCALI	2
Fluido eléctrico	3
Impresoras y Fotocopiadora	1
Red de datos (Intranet)	3

Nivel de Impacto: Alto = 3, Medio = 2, Bajo = 1

## **11. IDENTIFICACIÓN DE RIESGOS Y DEFINICIÓN DE PLANES DE CONTINGENCIA**

Se define como desastre a cualquier evento que pueda interrumpir el normal funcionamiento de las operaciones y/o servicios específicos.

Las personas que interviene en la ejecución del plan de contingencia, es la persona de sistemas, quien es el responsable de emitir la alarma de la falla e iniciar las actividades para la ejecución de la contingencia, apoyado por el jefe de Control Interno.

A continuación, se detallan los posibles escenarios que interrumpirían el normal desarrollo del funcionamiento de las operaciones y/o prestación de servicios específicos

### **11.1 PCs**

**Situación:** No enciende, Bloqueo, No navega

**Contingencia:** Para restablecer los PC, se deben seguir los siguientes pasos:

- Se reinicia el PC desde el botón de la carcasa.
- Se desconecta de la toma de energía y se vuelve a conectar.
- Se restablecen las copias de configuración almacenadas en los discos duros de la entidad
  1. DISCO DURO EXTERNO USB SIMPLE TECH Activo Fijo No 0515
  2. DISCO DURO USB HITACHI 2 TB Activo Fijo No 0532
  3. DISCO DURO USB EXTERNO 2.5" ADATA MODELO HD170 2 TB AF 0263

### **11.2 Fotocopiadora**

**Situación:** Falla en el servicio (Impresión, escaneo, fotocopias)

**Contingencia:**

1. Fotocopiadora en pantalla muestra error y su posible arreglo.
2. En caso de daño o un mal funcionamiento de la fotocopiadora, ABKA repara los equipos en días y horas hábiles de lunes a viernes de 08:00 a 12:00 y de las 14:00 a las 18:00 horas, los sábados de las 09:00 a las 13:00 horas.

Nivel de Soporte requerido	Tiempo de Respuesta
Soporte de primer nivel (telefónico a los usuarios)	Inmediata
Soporte de Segundo Nivel (de nuestros técnicos en sus instalaciones)	8 horas hábiles

En primera instancia el CIAC (Centro Integral de Atención al Cliente) está en la capacidad de guiarle en la solución inmediata del problema.

**11.3 Proveedor de Internet EMCALI**

**Situación:** Sin acceso a servicios de navegación

**Contingencia:** Se reinicia el modem provisto de emcali y se continúa con el soporte telefónico de emcali, línea 177. Soporte fibra Óptica, usuario:emru@dedicado.internet.

**11.4 Pagina Web**

**Situación:** Sin acceso a servicios de navegación

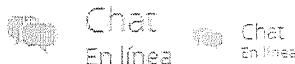
Contingencia: Se solicita soporte las 24 horas del día a:

Línea de soporte en la ciudad de Cali: (2)4858555

Línea Gratuita a nivel nacional: 018000120190

Página web: <https://www.colombiahosting.com.co/>


Icono



Si el plan de contingencia es ejecutado parcial o totalmente, es obligación del coordinador y/o técnico de sistemas, apoyado por su equipo de trabajo, realizar un análisis de las causas que ocasionaron la falla, presentar el respectivo informe a la gerencia y caso de ser necesario se realizara un plan de mejora.






	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

## 12. CENTRO DE SOPORTE

Cuando ocurra una falla que amerite la activación del plan de contingencia y el seguimiento a la atención del soporte es la siguiente:

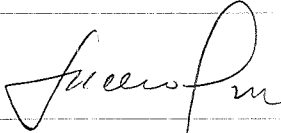
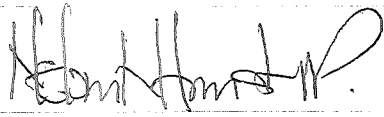
El usuario, si detecta la caída de sistemas debe solicitar visita presencial o enviar correo a soporte de la oficina de sistemas o al teléfono 6602560 – 62 si se realiza desde la sede CISO San Pascual.

ITEM	NOMBRE	CARGO	CORREO
1	OFICINA SISTEMAS	Soporte Técnico	harley.rodriguez@emru.gov.co
2	CONTROL INTERNO	Jefe Oficina Asesora Control Interno	controlinterno@emru.gov.co

	<b>MANUAL DE PLAN DE CONTINGENCIA INFORMATICA</b>	Código	PR-GO-25
		Versión	01
		Fecha	03-12-2018

### 13. CONCLUSIONES

Un Plan de Contingencia es la herramienta que cualquier empresa debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones.

	REVISO	APROBO
FIRMA		
NOMBRE	Lucero Mesa Naranjo	Nelson Londoño
CARGO	Jefe Administrativa y Financiera	Gerente
FECHA	03/12/18	03/12/18