Comisión de Regulación de Energía y Gas

PROCESO :	**INFORMÁTICA Y TECNOLOGÍA**
ACTIVIDAD :	**PLAN DE CONTINGENCIA INFORMÁTICO**
CÓDIGO :	**IT-PR-004**
VERSIÓN :	**2**

Elaboró:	**Revisó:**	**Aprobó :**
Asesor Informática y Tecnología	Comité de calidad	Comité de Calidad
Fecha: 25/01/2017	**Fecha:** 25/01/2017	**Fecha:** 07/03/2017

1. OBJETIVO

Establecer un plan de contingencia informático para los servicios de tecnología, que se prestan en la Entidad y que se pueda asegurar la continuidad del servicio.

2. ALCANCE

El alcance de éste procedimiento es para los servicios identificados como críticos de la infraestructura tecnológica de la CREG. Está dirigido a todo el personal involucrado en el proceso de Informática y Tecnología de la CREG.

3. GLOSARIO

- ✓ **CENTRO DE DATOS ALTERNO:** Es el Centro de datos encargado de absorber las operaciones del Centro de Datos Principal en caso de emergencia. Un centro de respaldo recibe estas denominaciones en función de su equipamiento

- ✓ **PLAN DE CONTINGENCIA:** Es un conjunto de procedimientos alternativos para activar el funcionamiento de los procesos de Informática y Tecnología cuando uno de sus servicios se afecta por un incidente interno o externo.

- ✓ **INCIDENTE:** Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo

4. ABREVIATURAS

- ✓ SAN: Unidad de almacenamiento (Storage Area network)

- ✓ Ups: Sistema de alimentación ininterrumpida (Uninterruptible Power Supply)

- ✓ Mpls: Enlace de datos (Multiprotocol Label Switching)

- ✓ Dns: Sistema para el manejo de nombres de dominio (Domain Name System)

- ✓ Dhcp: Protocolo para asignación de direcciones IP (Dynamic Host Configuration Protocol)

5. DESARROLLO

Se describirán los procedimientos alternos que se tienen a la operación normal, que le permiten a la Entidad seguir operando ante la eventualidad de una falla de los equipos y/o servicios que componen la plataforma tecnológica.

En caso de presentarse incidentes graves como explosiones, incendios, robos, que afecten en menor o mayor grado la operación de la Comisión de Regulación de Energía y Gas se ejecutará el procedimiento establecido para la activación del Data Center Alterno Sectorial del Ministerio de Minas y Energía y la CREG.

5.1 Políticas.

Mantener una Plataforma con características de redundancia y protegida por servicios en Garantía con el fabricante o convenios de mantenimiento.

Configurar en alta disponibilidad o en Cluster, en la medida que lo justifique el costo beneficio, los componentes que afecten servicios críticos.

Establecer procedimientos de contingencia independientes para cada uno de los servicios críticos.
Activar el Plan una vez se agoten los procedimientos normales de verificación y no haya sido posible la recuperación.

Asegurar la efectividad del sistema efectuando dos (2) pruebas independientes a lo largo del año de lo cual se dejará registro de ello en el Formato IT-FT-009 Registro pruebas Data Center Alterno. Las Pruebas se realizarán en horario hábil cuando se impacte menos la operación de la Entidad o en fines de semana.

5.2 Lineamientos.

Los servicios de tecnología no considerados como críticos deberán ofrecer mecanismos alternativos para su operación en caso de falla.
La prioridad de atención la tienen los servicios críticos alcance de éste procedimiento
La criticidad de los servicios puede variar en el tiempo.

5.3 Componentes del Plan

5.3.1 Servicios Críticos

	SERVICIO	SISTEMA
1	Portal de la Entidad	
2	Correo Electrónico	**Lotus Notes**
3	Sistema de Gestión Documental	**ORACULO**

4	Sistema de Información de Nómina	**SIGEP**
5	Controlador de Dominio	

5.3.2 Servidores

	SERVIDOR	FISICO	VIRTUAL	IP	SISTEMA OPERATIVO
1	CREGWEB		X	172.16.1.1	LINUX – CENTOS 6.3
2	CREGAS		X	172.16.1.7	LINUX – CENTOS 5.8
3	CREGBD	X		172.16.1.12	AIX 6.1
4	APOLO	X		172.16.1.16	AIX 7.1
5	IMÁGENES		X	172.16.1.98	Windows Server 2012 R2 Datacenter
6	DOMINIO		X	172.16.1.60	Windows Server 2008 R2 Enterprise

5.3.3 Equipos Activos

5.3.3.1 Switches Core

Los equipos core de red se encuentran conformados por dos switches capa 3 configurados en Stack y con fuente redundante. En caso que uno de los equipos presente falla, el otro equipo toma el control de la comunicación asegurando la continuidad de la operación. Los switches interconectan las fuentes de alimentación compartiéndolas como un recurso común que conforma el core unificando las fuentes de poder y dirigiendo el consumo de energía donde el sistema core lo requiera.

5.3.3.2 Switches de Borde

Los switches de borde se componen por 3 equipos conectados al core, por dos puertos uplink y se encuentran configurados en stack.

5.3.3.3 Switches SAN

Se cuenta con dos switches de SAN configurados en alta disponibilidad con todas sus conexiones en fibra.

5.3.4 UPS

La Entidad cuenta con un Sistema Ininterrumpido de Potencia UPS tipo paralelo 1+1, con capacidad 30KVA, 100% redundante. El tiempo de autonomía es de mínimo 20 minutos a plena carga, en caso que uno de los dos sistemas salga de operación se

garantiza un tiempo mínimo de 12 minutos.

5.3.5 Firewall

Se tiene configurado en cluster Activo, dos (2) equipos Firewall.

5.3.6 Canales de Internet

Para proporcionar el servicio de conexión a Internet se cuenta con un canal principal y un canal de respaldo ambos configurados en el Firewall para que en caso de caída de uno, el otro continúe proporcionando el servicio.

5.3.7 Canales de MPLS

Para proporcionar el servicio de conexión entre la sede principal y la de Combustibles Líquidos, se cuenta con un canal principal y un canal de respaldo, ambos configurados en el Firewall para que en caso de caída de uno, el otro continúe proporcionando el servicio.

5.3.8 Unidades de almacenamiento SAN

Se cuenta con dos unidades de almacenamiento SAN, una se encuentra configurada en replicación en línea con el Centro de Datos Alterno y adicionalmente con una segunda SAN ubicada en el Centro de datos Principal.

5.3.9 Sistemas de Información

a) Portal - CREGWEB
b) Aplicaciones Misionales Publicadas en el Portal – CREGAS
c) Nómina SIGEP
d) Correo Electrónico – APOLO
e) Sistema de gestión Documental ORACULO – APOLO
f) Normatividad y Jurisprudencia – APOLO
g) Servicios en Línea - APOLO
h) Herramienta para la Publicación de imágenes – IMÁGENES
i) Controlador de Dominio, DNS – DOMINIO

5.3.10 Datos

a) Base de Datos Oracle 10g – CREGBD
b) Data File de Imágenes y Máquinas virtuales - UNIDAD DE ALMACENAMIENTO SAN
c) SAN

5.4 Situaciones de Contingencia

5.4.1 Falla general de Data Center

En caso de presentarse fallo total del Centro de Datos Principal se debe seguir Protocolo de encendido, de acuerdo con las prioridades establecidas en el Anexo No. 1 - Protocolo de encendido/apagado, una vez se haya verificado el correcto funcionamiento de las UPS.

5.4.2 Falla del Suministro de Energía

En caso de presentarse falla eléctrica general entrará en operación la Planta eléctrica del edificio; durante ésta situación se debe monitorear el funcionamiento del Sistema de UPS para garantizar el suministro de la energía para los equipos de la Entidad y el centro de datos Principal.

Si se presenta falla con la Planta eléctrica del edificio entrará en operación el Sistema Ininterrumpido de Potencia UPS con la autonomía de mínimo 20 minutos a plena carga. En caso de falla de uno de los componentes del Sistema de UPS se debe contactar al proveedor contratado para hacer efectivo el protocolo de servicio técnico.

5.4.3 Falla en servidores

En caso de presentarse falla con un servidor de la Plataforma se identifica el alcance en los servicios que impacta y se activa la contingencia prevista para dicho equipo de acuerdo con los siguientes anexos:

- Anexo 2 – Relación de Servidores y su Contingencia
- Anexo 3 - Relación de servicios en ejecución por servidor

5.4.5 Falla en switches

En caso de presentarse falla con uno de los switches core o de borde se debe contactar al fabricante Cisco para hacer efectivo el protocolo de servicio técnico.

5.4.6 Falla en Firewall

En caso de presentarse falla con uno de los firewall del Cluster se debe contactar al proveedor contratado para hacer efectivo el protocolo de servicio técnico.

5.4.7 Falla en Canales de Internet y MPLS

En caso de presentarse falla con uno de los canales de acceso a internet o MPLS, se debe contactar al proveedor contratado para hacer efectivo el protocolo de servicio técnico.

5.4.8 Falla en unidades de almacenamiento SAN

En caso de presentarse falla con una de las SAN, se debe contactar al fabricante EMC para hacer efectivo el protocolo de servicio técnico.

5.4.9 Falla en Servicios

5.4.9.1 DNS

Para el servicio de resolución de nombres DNS se cuenta con los siguientes servidores:

SERVIDOR		DIRECCION IP	TIPO
DOMINIO	Primario	172.16.1.60	Virtual
CREGNET	Secundario	172.16.1.15	Virtual

Cada uno con su contingencia:

SERVIDOR		DIRECCION IP	TIPO
DOMINIO 1	Primario - Aislado	172.16.1.60	Virtual
CREGNET 1	Secundario - Aislado	172.16.1.15	Virtual

Con ésta configuración en caso de falla del servidor Primario DOMINIO resuelve el secundario CREGNET. En caso de falla de los dos servidores se activan sus contingencias virtuales.

5.4.9.2 DHCP

Para el servicio de asignación dinámica de direcciones (Dynamic Host Configuration Protocol) DHCP se cuenta con los siguientes servidores:

SERVIDOR	Servicio DHCP	DIRECCION IP	TIPO
DOMINIO	Activo	172.16.1.60	Virtual
CREGNET	Inactivo	172.16.1.15	Virtual

En el servidor CREGNET el servicio se encuentra Inactivo y se activa solo en caso de falla del servidor DOMINIO.

Cada uno con su contingencia:

SERVIDOR	Servicio DHCP	DIRECCION IP	TIPO
DOMINIO 1	Activo	172.16.1.60	Virtual
CREGNET 1	Inactivo	172.16.1.15	Virtual

Con ésta configuración en caso de falla del servidor DOMINIO se activa CREGNET y en caso de falla de los dos servidores se activan sus contingencias virtuales.

5.4.10 Falla en unidades almacenamiento

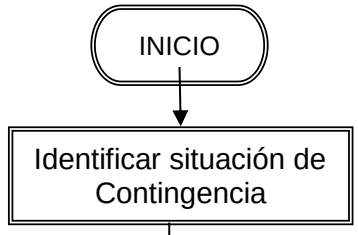
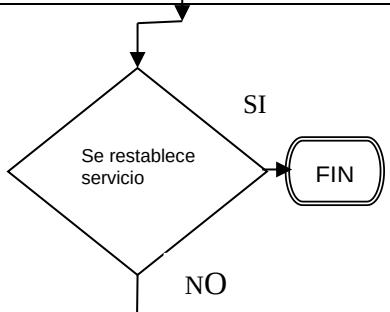
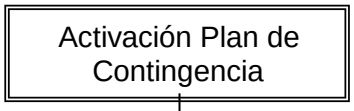
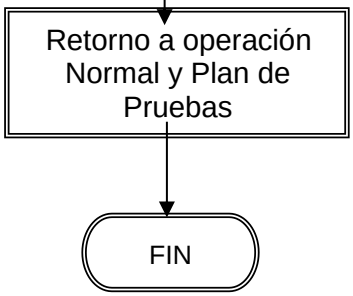
El servicio de almacenamiento de datos de la Entidad se encuentra centralizado en:

a) El Data File de Imágenes y Máquinas virtuales ubicado en la unidad de almacenamiento SAN.
b) SAN.

En caso de presentarse falla con uno de los dispositivos de almacenamiento se debe contactar al proveedor EMC para hacer efectivo el protocolo de servicio técnico.

En caso de presentarse problema con los datos por pérdida o corrupción de éstos se debe remitir al procedimiento IT-PR-001 Resguardo de información, para su restauración.

5.4. ACTIVIDADES.

No.	Etapa	Responsable	Documento	Descripción de la etapa
1.		Informática y Tecnología	N.A.	Se determina que se ha presentado una situación que genera interrupción de servicio crítico para la entidad.
2.		Informática y Tecnología	N.A.	Se restauran los servicios mediante los procedimientos normales
3.		Informática y Tecnología	N.A.	Se activa el Plan de Contingencia asociado al servicio crítico interrumpido
4.		Informática y Tecnología	N.A.	El servicio regresa al estado de operación normal.

6. CONTROL DE CAMBIOS

Descripción del cambio	Responsable	Fecha Modificación	Nueva Versión
Creación del documento.	**Medardo Rodríguez Becerra** Subdirector Administrativo y Financiero	11/02/2011	0
Modificación del documento	**Responsable Informática y Tecnología**	18/09/2013	1
Modificación del documento: Se realizan los cambios implicados por la entrada en operación de los canales MPLS, la adquisición de la SAN y el Centro de datos Alterno.	**Asesor IT**	07/03/2017	2

7. DOCUMENTOS RELACIONADOS

- ✓ IT-PR-001 Resguardo de información
- ✓ IT-FT-009 Registro pruebas Data Center Alterno

Comisión de Regulación de Energía y Gas

ANEXO No. 1
PROTOCOLO ENCENDIDO

#	SERVER	TIPO DE ENCENDIDO
1	DOMINIO	VMWARE
2	CREGNET	VMWARE
3	CREGBD	FISICO
4	APOLO	FISICO
5	ZEUS	FISICO
6	LOTUS TRAVELER	VMWARE
7	SAMETIME	VMWARE
8	IMÁGENES	VMWARE
9	IPSSERVER	VMWARE
10	CREGAS	VMWARE
11	POSEIDON	VMWARE
12	PERSEO	VMWARE
13	CREGWEB	VMWARE

PROTOCOLO APAGADO

#	SERVER	TIPO DE APAGADO
1	ZEUS	FISICO POR EL CLUSTER
2	APOLO	FISICO POR EL CLUSTER
3	LOTUS TRAVELER	VMWARE
4	SAMETIME	VMWARE
5	IPSSERVER	VMWARE
6	IMÁGENES	VMWARE
7	CREGAS	VMWARE
8	POSEIDON	VMWARE
9	PERSEO	VMWARE
10	CREGWEB	VMWARE
11	CREGBD	FISICO
12	DOMINIO	VMWARE
13	CREGNET	VMWARE

Comisión de Regulación de Energía y Gas

ANEXO No. 2

RELACION DE SERVIDORES Y SU CONTINGENCIA

NOMBRE SERVIDOR	DIRECCIÓN IP	NOMBRE SERVIDOR CONTINGENCIA
APOLO	172.16.1.16	ZEUS
CREGAS	172.16.1.7	CREGAS 1
CREGBD	172.16.1.12	Data Center Alterno
CREGNET	172.16.1.15	CREGNET 1
CREGWEB	172.16.1.1	CREGWEB 1
DOMINIO	172.16.1.60	DOMINIO 1
IMÁGENES	172.16.1.98	IMÁGENES 1
INTRACREG	172.16.1.36	INTRACREG 1
IPSSERVER	172.16.1.47	IPSSERVER 1
LOTUS TRAVELER	172.16.1.34	LOTUS TRAVELER 1
TRENDMICRO	172.16.1.14	TRENDMICRO 1

Comisión de Regulación de Energía y Gas

ANEXO No. 3
RELACION DE SERVICIOS EN EJECUCION POR SERVIDOR

#	NOMBRE DEL SERVIDOR	TIPO	APLICACIONES	SERVICIOS START
1	ABBY	Rack	Conversor de Imágenes	Servicio de conversion - ABBYCliente Tivoli RDP Servicio de archivos compartidos Windows HTTP Apache 2LogMeIn Conectores
2	CREGNET	Virtual	Activer directory, File Server, Controlador de Dominio Secundario	Active Directory WEB Services Group Policy Client Aranda Communicato Aranda Agent Client DHCP Administrador de discos logicos DNS Client DNS Conexiones de Red horario de Windows
3	CREGBI	Rack	Oracle 10g BI	Base de datos Oracle - CREGBI Cliente Tivoli RDP Servicio de archivos compartidos Windows
4	TRENDMICRO	Virtual	Antivirus Trend Micro, Office Scan	ntrtscanOfcAoSMgrShellHWDetectiontmlistenApache 2 TSM Client Acceptor TSM Client Scheduler W32 Time
5	IMÁGENES	Virtual	Imágenes Lotus	SrvImage - Servicio de publicacion de imágenes Cliente Tivoli RDP Servicio de archivos compartidos Windows
6	LOTUS TRAVELER	Virtual	Lotus Traveler, Sametime 8.0	dmserver Lotus Domino Diagnostics ((HLotusDomino) Lotus Domino Server (HLotusDominodata) TSM Client Acceptor TSM Client Scheduler W32Time
7	TSM - SERVER	Rack	Tivoli Storage Manager	Aranda Agent DB2DAS DB2DAS00 Servicio de gestion de DB2 (DB2TSM1) Servidor de mandatos remotos de DB2 (DB2TSM1) Tivoli Integrated portal V2.1_Tipprofile_port_16310DB2 DB2TSM1 Server1 terminal Services configurations storage manager 10 agent TSM client acceptor TSM client scheduler
8	ZEUS	Rack	Correo Lotus Notes 8.5.3 Aplicaciones Lotus CLUSTER	Aplicaciones Lotus Domino SMTP Lotus Domino POP3 Lotus Domino SSHSFTPHTTP Lotus Domino Cliente Tivoli NFS
9	IPSSERVER	Virtual	Compila, SAN, Aranda, WSUS	
10	VM_CLUSTER_1	Rack	Host 1 VM	N/A
11	VM_CLUSTER_2	Blade	Host 2 VM	N/A
12	VM_CLUSTER_3	Blade	Host 3 VM	N/A
13	DOMINIO	Virtual	Controlador Dominio Principal, DNS, DHCP, Active Directory	Active Directory WEB Services Aranda AgentDFS Namespacedfs Replication DHCP Client DHCP Server DNS Client group policy Client Kerberos Key Distribution center
15	APOLO	Rack	Correo Lotus Notes 8.5.3 Aplicaciones Lotus CLUSTER	Aplicaciones Lotus Domino SMTP Lotus Domino POP3 Lotus Domino SSHSFTPHTTP Lotus Domino Cliente Tivoli NFS
16	CREGAS	Virtual	Aplicaciones Web: Activos, cargos, compras, expansion, tarifas	SSHHTTp apache 2 HTTP Apache Tomcat - Puerto 8080 socket de carga Puerto 2001 Cliente Tivoli SFTP
17	CAMARAS / CONTROL ACCESO	Torre	Software de camaras y software de tarjetas de acceso	Alliance 8300 manager Alliance 8300 System Manager MSSQL SPQLW32 time
18	CREGWEB	Virtual	Portal WEB, Apache, MySQL, Joomla	base de datos MySQLCliente Tivoli RDP Servicio de archivos compartidos Windows Apache 2
19	CREGBD	Blade	oracle 10g Produccion	base de datos Oracle CREGBDClient Tivoli SSHSFTP
20	INTRACREG	Virtual	Intranet CREG	HTTP Apache 2 base de datos MySQLSSH Cliente Tivoli FTP Icecast Transmision de audio por broadcasting