**PLAN DE ACCION**

**NO COFORMIDAD AUDITORIA PVP**

**Riesgo**

Los riesgos ya se encuentran identificados en F-SG-03 para el área de IT. Y cubren diferentes aspectos relacionados con la seguridad informática.

**Descripción de la no Conformidad**

En la auditoria PVP se evidencia que aunque hay políticas para la seguridad informática, no hay planes de acción para atender adecuadamente los riesgos a la información.

**Acciones a realizar**

1. Documentar con un Manual, todos los procesos de contingencia informática que ya se realizan actualmente, a nivel detallado, las contingencias para cada uno de los riesgos identificados y sus responsables.

2. Realizar a partir de la fecha capacitaciones a los responsables e implicados en los procesos descritos.

3. Continuar mejorando y haciendo precisión sobre los detalles en este documento.

**MANUAL DE PLAN DE CONTINGENCIA**

**INFORMATICA**

|  |  |  |  |
| --- | --- | --- | --- |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** | |
| Firma  Nombre: Diego Agudelo, Diego Bernal  Cargo: Soporte Documental | Firma  Nombre: Diana Cristina Mesa  Cargo: Coordinadora SGI | Firma  Nombre: Juan Guillermo Galán  Cargo: Gerente General | |
| Fecha:13/12/2017 | Fecha:13/12/15 | Fecha: | |
| **CONTROL DE CAMBIOS** | | | |
| **ESTADO DEL DOCUMENTO** | **FECHA** | | **CAUSA DE CAMBIOS** |
| Versión 01 |  | |  |

**TABLA DE CONTENIDO**

[MANUAL DE PLAN DE CONTINGENCIA 2](#_Toc500941581)

[INFORMATICA 2](#_Toc500941582)

[1. INTRODUCCIÓN 4](#_Toc500941583)

[2. GENERALIDADES 4](#_Toc500941584)

[2.1. DEFINICIONES 4](#_Toc500941585)

[3. OBJETIVO GENERAL 4](#_Toc500941586)

[4. OBJETIVOS ESPECÍFICOS 5](#_Toc500941587)

[5. ALCANCE Y RESPONSABILIDADES 5](#_Toc500941588)

[6. TIEMPO DE INACTIVIDAD 5](#_Toc500941589)

[7. DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS 6](#_Toc500941590)

[8. PLATAFORMA DE SOPORTE IT 6](#_Toc500941591)

[9. ANÁLISIS DE RIESGOS 7](#_Toc500941592)

[10. EVALUACIÓN Y CALIFICACIÓN DEL IMPACTO DE LOS PROCESOS CRÍTICOS PARA LA CONTINUIDAD DEL SERVICIO 7](#_Toc500941593)

[11. ESTRUCTURA DE LA RED DE INFORMACIÓN 8](#_Toc500941594)

[12. IDENTIFICACIÓN DE RIESGOS Y DEFINICIÓN DE PLANES DE CONTINGENCIA 9](#_Toc500941595)

[13. CADENA DE ESCALAMIENTO SEGÚN LA FALLA 13](#_Toc500941596)

[14. PLATAFORMA SATLOCK 14](#_Toc500941597)

# INTRODUCCIÓN

Los sistemas de información son parte esencial en el funcionamiento del negocio, es por esto que debemos estar preparados ante todos los posibles riesgos, para esto es conveniente procedimientos y acciones básicas de respuesta que se debería tomar para afrontar de manera oportuna, adecuada y efectiva, la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir.

Durante el desarrollo del plan de acción se toman unas medidas necesarias los cuales nos ayudan a ejercer un mayor panorama cuando se nos puedan presentar algún problema, de tal manera que se realizan protocolos o normas las cuales debemos seguir para tener su respectiva solución en el menor tiempo posible o en el tiempo estipulado.

# GENERALIDADES

2.1. DEFINICIONES

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

# OBJETIVO GENERAL

Garantizar la continuidad del servicio en las áreas más críticas de nuestra operación, para la empresa SATLOCK S.A.S, con fines restaurar la operación en los tiempos oportunos para su funcionamiento.

# OBJETIVOS ESPECÍFICOS

4.1. Garantizar las operaciones del negocio en todas las áreas de la empresa.

4.2. Realizar acciones pertinentes y minimizar el riesgo de caídas constantes de servidores.

4.3. Proteger la información ante un uso inadecuado de la información o de sitios inseguros.

4.4. Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.

# ALCANCE Y RESPONSABILIDADES

El Director de ingeniería o coordinador IT es el responsable de la ejecución del plan de contingencia con el apoyo de los funcionarios de la empresa a quienes hacen uso de los recursos informáticos.

# TIEMPO DE INACTIVIDAD

El término tiempo de inactividad es usado para definir cuando el sistema no está disponible (solo para servidores). Los casos pueden ser planeados o no planeados.

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, daño en los servidores, fallas de la red de datos, fallas en el fluido eléctrico.

# DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS

|  |  |  |
| --- | --- | --- |
| RECURSO | PROBLEMA RELACIONADO (RIESGO ASUMIDO) | |
| POSIBILIDAD DE  OCURRENCIA DEL PROBLEMA | PERIODO DE PARA ACEPTABLE |
| PC | BAJA | 1 DIA |
| SISTEMA DE  INFORMACIÓN | BAJA | 2 HORAS |
| SERVIDORES | BAJA | 2 HORAS |
| IMPRESORA | MEDIA/ALTA | 6 HORAS |
| TELÉFONO IP | MEDIA/ALTA | 4 HORAS |

# PLATAFORMA DE SOPORTE IT

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

8.1. Computador de Escritorio y Portátil:

Se cuentan con equipos de cómputo de marca HP, TOSHIBA, LENOVO Y DELL de varias referencias, Adicionalmente unos equipos arrendados.

8.2. Impresoras

Se cuentan con impresoras láser de mediano y alto rendimiento y con impresoras de inyección de tinta de bajo rendimiento.

8.3. Página Web Soporte

Se Cuenta con una página web la cual puede subir su ticket ante cualquier eventualidad a la caída o daño de algún recurso.

8.4. Teléfonos IP

Se cuenta con teléfonos de Voz – ip marca GRANDSTREAM.

# ANÁLISIS DE RIESGOS

|  |  |  |
| --- | --- | --- |
| OPERACIÓN | CONTENIDO DE LA  OPERACIÓN | PRIORIDAD DE LA  OPERACIÓN |
| Programas | Netsolin  Antares  Satlockonline | ALTA |
| Comunicaciones | Telefonía IP  Internet y Correo. | ALTA |

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

|  |  |
| --- | --- |
| RECURSOS | NIVEL DE IMPACTO |
| Servidores | 3 |
| Sistema de Información | 2 |
| Página WEB | 3 |
| Teléfono IP | 2 |
| Internet | 3 |
| Fluido eléctrico | 2 |
| Impresoras | 1 |
| Red de datos | 3 |

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

# ESTRUCTURA DE LA RED DE INFORMACIÓN

11.1. TIPO DE EQUIPO: Servidor Físico

ESPECIFICACIONES TÉCNICA

Marca : HP

Modelo : Proliant ML 110 G6

Procesador : Intel Xeon 2.0 GHz

Memoria RAM : 16 GB

Disco Duro : 976 GB

Sistema Operativo: Windows Server 2008 Stándard

Nombre : STLSERVER1

SERVICIOS SOPORTADOS:

Sistema integral de información

DHCP

Proxy

Hosting

FTP

TABLEAU

TIPO DE EQUIPO: Servidor Físico

ESPECIFICACIONES TÉCNICA

Marca : Lenovo

Modelo : Thinkserver TS150

Procesador : Intel Xeon 3.3 GHz (4 Núcleos)

Memoria RAM : 16 GB

Disco Duro : 802 GB

Sistema Operativo: Windows Server 2012R Standard

Nombre: Servidor Satlock.

SERVICIOS SOPORTADOS:

Sistema integral de información

PBX Cali

Antares

Netsolin

FTP

TIPO DE EQUIPO: Servidor Físico

ESPECIFICACIONES TÉCNICA

Marca :DELL

Modelo : PowerEdge 1850

Procesador : Intel Xeon 2.8 GHz

Memoria RAM : 2 GB

Sistema Operativo: Centos 5.8

Nombre : vozip

SERVICIOS SOPORTADOS:

PBX BOGOTA

# IDENTIFICACIÓN DE RIESGOS Y DEFINICIÓN DE PLANES DE CONTINGENCIA

Las personas que interviene en la ejecución del plan de contingencia, es el personal de sistemas, en cabeza del Director de Ingenieria o el Coordinador IT, quien es el responsable de emitir la alarma de la falla e iniciar las actividades para la ejecución de la contingencia.

.

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

## Servicios

### Situación: Falla del servidor STLSERVER1.

Falla total o parcial del hardware o software del servidor

Contingencia:

Para restablecer los servicios de DHCP, PROXY, HOSTING Y FTP, se deben seguir los siguientes pasos:

1. Se verifica si el servidor denominado *STLSERVER1 esta encendido.*

2. Se conecta una pantalla y un teclado

3. Se reinicia el servidor

4. Se verifica la configuración y el modo de encendido

Tiempo aproximado: 30 minutos

Recursos: Personal Humano de la oficina de sistemas

### Situación: Falla del servidor denominado ServidorSatlock

Para restablecer el servicio de Tableau, Antares y PBX se hace lo siguiente.

Contingencia:

1. Se verifica que el ServidorSatlock este encendido

2. Se ingresa de manera remota por medio de VMware

3. Se revisa que las máquinas virtuales estén encendidas.

4. Se hace un reinicio de la Maquina que tenga la Afectación.

5. Se Verifica el funcionamiento de equipo si tiene algo que sea anormal.

6. Si no funciona esto se hace un reinicio físico de la máquina para que se ejecute todo normalmente.

Tiempo aproximado: 40 minutos.

Recursos: Personal Humano de sistemas.

### Situación: Falla Del Servidor Denominado Vozip

Para Restablecer el servicio de Llamadas Telefónicas física mente o Virtualmente, hacemos lo siguiente.

Contingencia:

1. Cuando es virtual se hace conexión a la VPN de la Oficina.

2. Se ingresa a la IP del servicio.

3. Ingresamos al Flash Operator Panel y verificamos si hay caída de una troncal o extensión.

4. Se ejecuta el comando core restar gracefully.

5. Se Verifica el funcionamiento de equipo.

6. Si no funciona se ejecuta el comando de reinicio total.

Tiempo aproximado: 30 minutos.

Recursos: Personal Humano de sistemas y Teléfono Celular.

### Situación: Caída de Energía en Bogotá

Restablecer el servicio de energía se hace lo siguiente

Contingencia:

1. Dos Ups que mantienen la alimentación mientras la transferencia automática de la planta inicia la planta.

2. Una transferencia automática que no requiere intervención humana.

3. Un instructivo de uso manual de la planta

Tiempo aproximado: 5 minutos.

Recursos: Personal Humano de Sistemas

### Situación: Caída Energía en Cali

Restablecer el servicio de energía se hace lo siguiente

Contingencia:

1. Dos Ups que mantienen la alimentación mientras la transferencia automática de la planta inicia la planta.

Tiempo aproximado: 10 minutos.

Recursos: Personal Humano de sistemas.

### Situación: Caída o Falla de Internet en Bogotá

Restablecer el servicio de internet se hace lo siguiente

Contingencia:

1. Un canal alterno con proveedor diferente, disponible en todo momento.

Tiempo aproximado: 10 minutos.

Recursos: Personal Humano de sistemas y Teléfono Celular.

### Situación: Caída o Falla de Internet en Cali

Restablecer el servicio de internet se hace lo siguiente

Contingencia:

1. Se instalan modem en los pc de Monitoreo

2. Le hago ping sostenido a la ip

3. Llamo a Cali y pido que me revisen la conexión.

4. pido que me reseteen el cisco

5. Llamo a claro

Tiempo aproximado: 30 minutos.

Recursos: Personal Humano de sistemas.

### Situación: Ataque de Virus en Equipo

Recuperar la mayor cantidad de información posible.

Contingencia:

1. Se aísla de inmediato de la red

2. Se deshabilitan los adaptadores de red

3. Se ejecuta un antivirus tratando de identificar el problema.

4. Si el problema es mucho más grabe se formatea el equipo

5. Introducimos el Backup que está alojado en el servidor denominado STLSERVER1, en el disco quinto, en la carpeta backup.

6. Descargamos el backup al que es asociado para esta persona, el cual esta encriptado con una contraseña.

7. por último descargamos el backup.

Tiempo aproximado: 2 días.

Recursos: Personal Humano de sistemas.

# CADENA DE ESCALAMIENTO SEGÚN LA FALLA

Cuando ocurra una falla que amerite la activación del plan de contingencia la cadena de llamado será la siguiente

El usuario final, si detecta la caída de sistemas debe llamar al teléfono de soporte

Que se ha avisado en un plan de acción ante cualquier novedad.

La prioridad de llamada se puede dar del siguiente modo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ITEM | NOMBRE | CARGO | TELÉFONO | FALLO EN |
| 1 | Diego Bernal | Auxiliar de Ingenieria | 3234838947 | PBX, CANALES DE INTERNET, COMPUTADORES, PAGINA COMERCIAL, CORREOS ELECTRONICOS, LINEAS TRANSACCIONALES |
| 2 | Diego Agudelo | Director de Ingenieria | 3106537783 | PLATAFORMA SATLOCK |

# PLATAFORMA SATLOCK

La plataforma SATLOCK se encuentra alojada en servidores con el proveedor Grandeservers, el cual nos brinda bajo contrato unos niveles de acceso del 99.9%.

Está conformado por servidores físicos, la base de datos, y un conjunto de servidores virtuales, con sistemas opertivos Linux y windows, especializados en diferentes aspectos del negocio.

A continuación se describen los posibles esenarios que se pueden presentar, y el proceso que se revisa.

**Carga de Base de Datos:**

Se genera ante un pico de procesamiento de información, o algunas consultas largas.

Proceso de recuperación:

* Se procede a correr el script para identificar las cosultas demoradas.
* Se bajan los interpretadores por uno o dos minutos, se reinician nuevamente.
* Si las consultas cargadas corresponde a VACUUM se procede a cancelarlas.
* Se corren el script relacionado con mantenimiento de tablas administrativas.
* Si la consulta corresponde a un reporte muy largo, se procede a terminarla individualmente.

Responsable

* Ingeniería.

**Corrupción de la Base de Datos:**

Alguna de las tablas está corrupta.

Proceso de recuperación:

* Se restablece la tabla dañada desde el backup realizado el día anterior.

Responsable

* Ingeniería

**Mal funcionamiento Máquina Virtual:**

Las máquinas virtuales podrían llegar a sufrir corrupción en sus datos, y las aplicaciones comenzar a fallar.

Proceso de recuperación:

* Se contacta con el proveedor Grandeservers para iniciar el restablecimiento de una maquina Snapshot de la máquina afectada.
* Se cambian los direccionamientos a la máquina nueva.
* Se verifica el funcionamiento correcto de la aplicación afectada.

Responsible

* Ingeniería en conjunto con el proveedor.

**Falla en conectividad:**

El proveedor pierde su canal de internet.

Proceso de recuperación:

* Se contacta al proveedor Grandeservers para que realice sus contactos al Datacenter y se restablezca la conectividad.
* Se realizan la pruebas y se hace seguimiento.

Responsible:

* Ingeniería en conjunto con el proveedor.

**Carga en servidor de interpretadores:**

Aparece carga en el servidor de interpretadores que ralentiza los procesos.

Proceso de recuperación:

* Se listan las tareas del servidor y se ordenan descendentemente por consumo de CPU.
* Si uno de los interpretadores está generando una sobre carga, se reinicia ese proceso.
* Se listan los procesos por consumo de memoria RAM.
* Si uno de los interpretadores, tiene sobreconsumo se reinicia ese proceso.