**PLAN DE CONTINGENCIA Y POLITICAS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DE LA INSTITUCIÓN TECNOLOGICA COLEGIO MAYOR DE BOLIVAR**

OBJETIVO

Describir una estrategia planificada compuesta por un conjunto de procedimientos alternativos a la operatividad normal en la ITCMB los cuales permitan y garanticen la continuidad del funcionamiento de los sistemas de información durante y después de la materialización de una amenaza interna o externa.

FASES PARA LA LABOR DE CONTINGENCIA FASE

I. PLANEACIÓN

1. Diagnostico

Para determinar las acciones a llevar a cabo, es necesario contar con un panorama de los recursos que la Institución utiliza y el grado de importancia de acuerdo al nivel de complejidad y transacción de datos.

- SERVIDORES
- SOFTWARE
- MAQUINAS VIRTUALES
- EQUIPOS DE CÓMPUTO Y PARTES
- INTERNET
- REDES Y EQUIPOS ACTIVOS

2. ANALISIS DE RIESGOS

- Riesgos por Fallas Humanas
- Riesgos por Fallas Técnicas
- Riesgos por falta en el suministro de servicios públicos
- Riesgos Catastróficos/Naturales
- Riesgos Ambientales

ESTRATEGIA TECNOLOGICA SERVIDOR BLADE HP No. 4

1. OBJETIVO

Recuperar el servidor Blade Hp principal por daño en alguno de los servicios soportados o en el hardware.

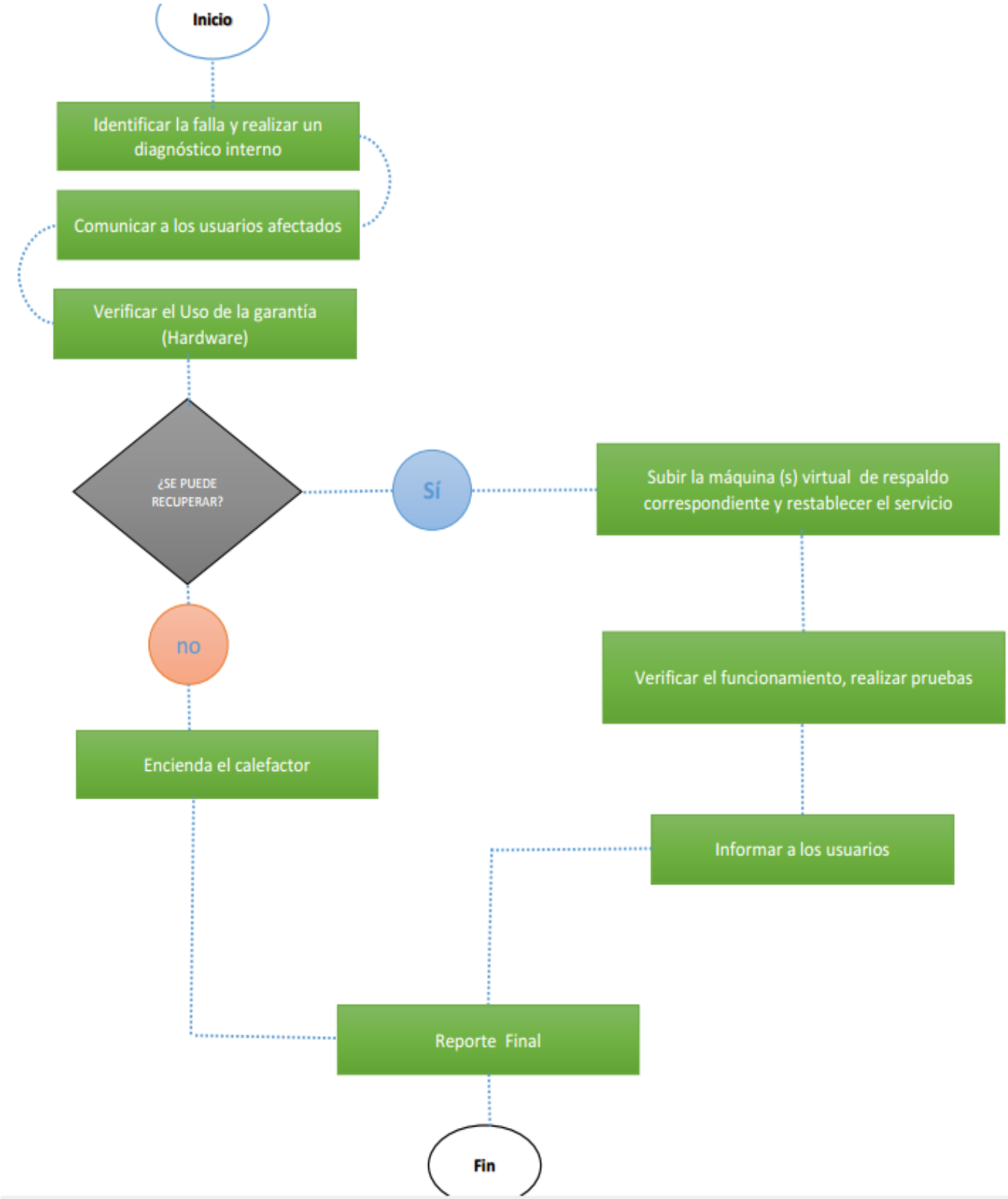
2. ALCANCE

El procedimiento aplica para los siguientes escenarios:

- Daños o fallas en algún servicio que afecte las funciones y/o actividades que se ejecutan a diario en la ITCMB por los empleados.
- Falla a nivel de hardware en el servidor.

3. DESCRIPCIÓN

DIAGRAMA DE FLUJO



ACTIVIDADES O TAREAS

| No. Act | Actividad o tarea | Descripción | Responsable | Recursos |
|---|---|---|---|---|
| 1 | identificar la falla y realizar un diagnóstico interno | Identificar el tipo de falla | Personal de soporte y/o Jefe de unidad | Humano |
| 2 | Comunicar a los usuarios afectados | Dar a conocer a los usuarios de la mejor manera como está la situación (tiempos de solución) | Personal de soporte y/o Jefe de unidad | Chat, teléfono, correos, página web |
| 3 | Verificar el Uso de la garantía (Hardware) | Si ésta existe proceder, de lo contrario buscar la pieza con los proveedores | Personal de soporte y/o Jefe de unidad | Contrato garantía |
| 4 | SE PUEDE RECUPERAR? | Si la respuesta es positiva continuar con el paso siguiente (5), de lo contrario ir al paso 8 | | |
| 5 | Subir la máquina (s) virtual de respaldo correspondiente y restablecer el servicio | Si el daño es en alguna máquina virtual o en algunos de sus servicios, esto mientras se resuelve el problema | Personal de soporte y/o Jefe de unidad | Equipo servidor de respaldo |
| 6 | Verificar el funcionamiento, realizar pruebas | Se verifica que el servicio y la operación ese encuentren en su estado normal | Personal de soporte y/o Jefe de unidad | Humano, equipos pc, servidor de respaldo |
| 7 | Informar a los usuarios | Se informa a los usuarios para que realicen las respectivas pruebas | Personal de soporte y/o Jefe de unidad | Chat, teléfono, correos, página web |
| 8 | Reporte | El coordinador encargado informar de manera formal la situación y la solución o no de ésta | Jefe de unidad | Correo |

POLITICAS

Es compromiso de todos y cada una de los usuarios de los sistemas de información de la ITCMB conocer y acatar las siguientes políticas durante el desarrollo de sus funciones.

1. **Política:** Protección de recursos informáticos

   1.1 El usuario o funcionario deberán reportar de forma inmediata a la oficina sistemas informáticos cuando se detecte algún riesgo real o potencial sobre equipos de cómputo o de comunicaciones, tales como caída de agua, choques eléctricos, caídas, golpes o peligro de incendio.

   1.2 El usuario o funcionario tiene la obligación de proteger cualquier activo o recurso de información que se encuentren bajo su responsabilidad como torres, equipos portátiles, mouse, teclado, pantalla, tarjetas externas, unidades de almacenamiento etc.

   1.3 Los equipos de cómputo y cualquier activo de información, podrá ser retirado de las instalaciones de la ITCMB únicamente con la debida autorización del área de sistemas informáticos.

   1.4 Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mimos sin autorización de la oficina de sistemas informáticos, en caso de requerir cualquiera de estos servicios deberá ser solicitado por medio de la mesa de ayuda o sistema de tickets.

   1.5 Es responsabilidad de cada usuario no consumir ningún tipo de alimentos o bebidas en el lugar donde se encuentra el equipo de cómputo o cualquier otro recurso informático.

   1.6 Solo el personal de la oficina de sistemas informáticos son los únicos autorizados para abrir, destapar y realizar cualquier clase mantenimiento a los equipos de cómputo y cualquier otro recurso informático.

2. Política: Gestión de software

   2.1 Ningún usuario, funcionario, empleado o personal externo, podrá descargar programas (software) sin la debida autorización de la oficina de sistemas informáticos.

2.2 Los usuarios y/o funcionarios no pueden instalar ni desinstalar ningún tipo de programa (software), no pueden realizar modificaciones ni alteraciones a la configuración establecida de los programas, sistema operativo y SetUp de la Bios en sus computadoras ni en ningún otro recurso informático sin antes no estar autorizado por la oficina de sistemas informáticos.

2.3 Cualquier usuario que vea o sospeche de alguna infección por malware en su computadora, deberá notificar inmediatamente a la oficina de sistemas informáticos para la respectiva revisión y no realizar ninguna acción.

3. Política: Gestión de cuentas de correo electrónico

3.1 Los usuarios o funcionarios no deberán utilizar sus cuentas de correos asignadas para uso personal, los mensajes de correo electrónico y archivos adjuntos son de propiedad de la ITCMB

3.2 Los usuarios o funcionarios son los responsables de la descarga de los archivos adjuntos de sus cuentas de correos, si tienen alguna duda de la procedencia de algún correo se recomienda no descargar ni abrir el adjunto, para estos casos se debe informar a la oficina de sistemas informáticos quienes están en la obligación de apoyar.

4. Política: Gestión de Redes e Internet

4.1 El acceso a Internet proporcionado a los usuarios y funcionarios de la ITCMB es exclusivamente para las actividades relacionadas con las funciones del cargo y las desempeñadas, por lo tanto habrá restricciones en el acceso algunas páginas, esto con el fin de evitar cualquier tipo de problema relacionados a infecciones de malware, consumo del ancho de banda, bloqueos de sistema operativo, entre otros tipos de problemas.

4.2 Cada usuario o funcionario deberá solicitar a la oficina de sistemas informáticos, con el aval de su jefe inmediato, el acceso a páginas con restricción.

4.3 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provisto por la ITCMB, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por la oficina de sistemas informáticos.