	<b>Documento General:</b>	Código	CHAD-SI-DG-02
	<b>PLAN DE CONTINGENCIA</b>	Versión:	00
		F. Emisión:	17/10/2016

## **Objetivos**

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la compañía, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna.

## **Descripción de las Operaciones**

El plan de contingencia se aplica a todos las PC's y Servidores de la empresa. En el cual se detallara los procedimientos que se aplicaran a los diferentes equipos.

Además de las posibles fallas a presentar y medidas a tomar por el responsable del área de sistemas.

## **Responsables del plan de contingencia**

Coordinador de Sistemas

Utilizara un monitor y un mouse para apagar los servidores en caso de que el ups se quede sin batería.

En caso que no se encuentre el Coord. De Sistemas , se llamara al proveedor del servicio.

## **Descripción de las Contingencias**

### **Corte del Fluido Eléctrico**

#### **Medidas de Seguridad**

Como medida de seguridad los Servidores están conectados a un equipo que le dará corriente por un tiempo determinado en caso de corte en el fluido eléctrico.


#### **Pasos a seguir en caso de corte del Fluido Eléctrico**

A continuación se mencionan los pasos a seguir cuando se produzca un corte en el fluido eléctrico:

- ☐ El UPS da a los Servidores, corriente por un tiempo de 30 minutos, por lo tanto se tiene éste lapso para apagarlo sin problemas. El software instalado en el servidor bajará el sistema en caso no se pueda realizar manualmente.
- ☐ Para apagar los Servidores existen dos formas seguras, sea ésta localmente ó remotamente, a continuación son mencionadas:

#### **Forma # 1:**

<b>Elaboración:</b>	<b>Revisión:</b>	<b>Aprobación:</b>
Diego Centeno Auxiliar de Sistemas Fecha: 13/10/2016	Rossana Delgado Coordinador del SGI Fecha: 14/10/2016	Percy Napurí Gerente General Fecha: 17/10/2016
<b>Prohibido imprimir, fotocopiar o reproducir este Documento</b>		

	<b>Documento General:</b>	Código	CHAD-SI-DG-02
	<b>PLAN DE CONTINGENCIA</b>	Versión:	00
		F. Emisión:	17/10/2016

- Realizar el siguiente comando:
- Init 0 y ENTER.

#### **Forma # 2:**

- Tambien se puede realizar el siguiente comando:
  - Shutdown y ENTER
- ❑ Lo más seguro es que las PC's hayan quedado encendidas, se debe recorrer las estaciones apagando/desactivando el botón de encendido y supresores de pico, esto para evitar que se dañen los equipos cuando el fluido se restablezca.
- ❑ Se recomienda apagar todas las luces en caso fuera de día y en el caso de noche o de poca visibilidad sólo las luces de los pasadizos deben ser encendidas. Evitar el uso de la fotocopiadora.

### **Fallas en los Equipos**

#### ***Medidas de seguridad***

Los equipos asignados al personal de CHOICE ADUANAS se encuentran en perfecto estado, las configuraciones son las adecuadas para su mejor funcionamiento y los sistemas instalados son los necesarios para el desarrollo de las actividades laborales.

#### **1. Posibles causas de las fallas**

Una de las posibles causas para la desconfiguración de los Equipos se da al apagar la PC. Para cerrar la sesión en el Sistema Operativo Windows, se debe realizar un proceso, cuando no se realiza éste correctamente y se apaga bruscamente la máquina se dañan o pierden archivos ocasionando fallas en los equipos.


Otro motivo para que falle una PC se produce al instalar un software sin los parámetros adecuados, este paso está cubierto por el Dpto. de Sistemas.

También se producen fallas debido a la carga de trabajo de los componentes de la PC.

#### **2. Si la máquina no puede conectarse a Red**

- ◆ En primer lugar verificar que el Login y el Password sean los correctos.
- ◆ Si el problema persiste verificar que los cables de red estén correctamente conectados.
- ◆ Verificar en el Switch que el cable este correctamente conectado.
- ◆ Hacer pruebas de conexión cambiando de ubicación el punto en el Switcher.
- ◆ Si el problema persiste es probable que haya conflicto en la Configuración de la Tarjeta de Red. Existe un archivo con configuraciones éste debe ser consultado y escoger la configuración disponible y adecuada para ese equipo.
- ◆ Si no se solucionó el problema posiblemente la tarjeta de Red deba ser cambiada.

<b>Elaboración:</b>	<b>Revisión:</b>	<b>Aprobación:</b>
Diego Centeno Auxiliar de Sistemas Fecha: 13/10/2016	Rossana Delgado Coordinador del SGI Fecha: 14/10/2016	Percy Napurí Gerente General Fecha: 17/10/2016
<b>Prohibido imprimir, fotocopiar o reproducir este Documento</b>		

	<b>Documento General:</b>	Código	CHAD-SI-DG-02
	<b>PLAN DE CONTINGENCIA</b>	Versión:	00
		F. Emisión:	17/10/2016

### 3. Cuando el equipo presenta fallas

Dependiendo de la gravedad del problema se pueden realizar los siguientes procesos:

- ☐ Realizar el proceso de respaldo de los documentos y las carpetas personales y Formatear el disco duro e instalar nuevamente todos los sistemas, realizando las configuraciones tanto de Software como de Hardware.
- ☐ Si el problema persiste es muy probable que el equipo deba ser cambiado.

### Infección de Virus en una Estación

#### **Medidas de Seguridad**

Para evitar que las máquinas sean infectadas con Virus se ha instalado en cada una un Software de Seguridad contra Virus, también llamado Antivirus, este programa se encuentra en modo residente, es decir se encuentra activo durante toda la sesión con la finalidad de examinar en tiempo de ejecución los archivos que se estén ejecutando y los que se encuentren almacenados en el Disco Duro.

Se ha instruido al personal de CHOICE ADUANAS de no abrir ningún mensaje de correo electrónico en el que el DESTINATARIO sea desconocido o que el ASUNTO tenga algo de extraño, los Usuarios deben de notificar inmediatamente al personal de Tecnología de la información para la revisión correspondiente.

**Los antivirus se actualizan todos los días de forma Automática.**

#### **Indicios de que la estación tiene Virus**

Cuando una Estación está infectada con algún Virus informático presenta una manera extraña de funcionamiento dependiendo de las características del Virus.

Existen virus que afectan el sistema de arranque de la máquina evitando que ésta inicie la sesión, otros al ejecutarse eliminan información del Disco Duro, existen virus que al infectar una estación presentan una dirección electrónica en la que se puede adquirir la vacuna. Como se puede apreciar los virus afectan de diferentes maneras el funcionamiento de las estaciones.


Se recomienda notificar al Dpto. de Sistemas cuando las Estaciones presenten funcionamiento extraño para que se realice el proceso conveniente de desinfección.

### 1. Cuando la Estación está infectada.

En el caso de que algún Virus logre evadir el Software de seguridad se deben seguir los siguientes pasos:

- ☐ Desconectar la estación de la Red para evitar que el virus llegue al Servidor e infecte otras estaciones.
- ☐ Conseguir la actualización del Antivirus o de lo contrario otro software más actualizado.
- ☐ Desinfectar la estación.

<b>Elaboración:</b>	<b>Revisión:</b>	<b>Aprobación:</b>
Diego Centeno Auxiliar de Sistemas Fecha: 13/10/2016	Rossana Delgado Coordinador del SGI Fecha: 14/10/2016	Percy Napurí Gerente General Fecha: 17/10/2016
<b>Prohibido imprimir, fotocopiar o reproducir este Documento</b>		

	<b>Documento General:</b>	Código	CHAD-SI-DG-02
	<b>PLAN DE CONTINGENCIA</b>	Versión:	00
		F. Emisión:	17/10/2016

- ☐ Revisar los archivos para determinar las pérdidas de información.
- ☐ Utilizar la última copia de seguridad para actualizar la información.
- ☐ Realizar las pruebas necesarias y conectar la estación a la Red.

## 2. Cuando el Servidor está infectado con Virus

- ☐ Las medidas a tomar deben ser inmediatas y muy precisas.
- ☐ En primer lugar se debe tener la copia de seguridad en este caso en un Disco Duro Externo.
- ☐ El Servidor debe ser reemplazado para que los usuarios continúen trabajando hasta que se realice la desinfección.
- ☐ Lo más probable es que algunas estaciones estén infectadas, por tal motivo antes de continuar con los procesos se debe pasar el antivirus a todas las estaciones.
- ☐ Conseguir la actualización del Antivirus o de lo contrario otro software más actualizado.
- ☐ Pasar el antivirus al Servidor seleccionando las opciones de mayor limpieza y detección de virus.
- ☐ Realizar un nuevo diagnostico al servidor.
- ☐ Consultar a los usuarios sobre la información perdida y restaurarla del Back up.
- ☐ Una vez probado el Servidor y confirmar que está desinfectado, se instala nuevamente a la Red.


## 3. Cuando Ningún Servidor responda

- ☐ Se solicitara a nuestro proveedor de confianza un Servidor lo antes posible.
- ☐ Copiar los Datos del Sistema del Disco Duro Externo en el nuevo Servidor y configurarlo.
- ☐ Conectarla a la Red para que entre en Producción nuevamente y la empresa no se paralice.
- ☐ Enviar los Servidores averiados al servicio técnico para las soluciones respectivas.

## 4. En caso de desastre de la infraestructura

- ☐ El personal comercial, contable, sistemas y operativo calificado deberá ir a las oficinas destinadas por la organización CHOICE ADUANAS.
- ☐ Se realizará un contrato de alquiler de computadoras y servidores a nuestros proveedores a fin de tener nuevamente infraestructura tecnológica para el desarrollo de los procesos.
- ☐ El Dpto. de Sistemas configurará las nuevas cuentas de acceso y de correo electrónico a fin de que tengan las herramientas para seguir con los procesos del negocio.

<b>Elaboración:</b>	<b>Revisión:</b>	<b>Aprobación:</b>
Diego Centeno Auxiliar de Sistemas Fecha: 13/10/2016	Rossana Delgado Coordinador del SGI Fecha: 14/10/2016	Percy Napurí Gerente General Fecha: 17/10/2016
<b>Prohibido imprimir, fotocopiar o reproducir este Documento</b>		

	<b>Documento General:</b>	Código	CHAD-SI-DG-02
	<b>PLAN DE CONTINGENCIA</b>	Versión:	00
		F. Emisión:	17/10/2016

- ❑ Se copiará la información del último backup en los nuevos servidores para que los sistemas estén completamente actualizados.

### **Respaldo de la información (Backup)**

#### **• Copias de seguridad**

- ❑ Se realiza una Copia de Seguridad de los Datos del Sistema en un Disco Duro Externo, el cual estará guardado en Sala de Servidores.
- ❑ Se realiza otra Copia de Seguridad de los Datos del Sistema en un Disco Duro Externo el cual se mantendrá fuera de las instalaciones de Choice Aduanas por seguridad.

#### **• Restauración de Backups**

##### **DATOS**

- ❑ El Coordinador de Sistemas, semanalmente envía al proveedor del sistema operativo, copia del backup realizado.
- ❑ El proveedor, verifica la idoneidad del backup, verificando que la información enviada, se encuentre en correcto funcionamiento.
- ❑ El proveedor, emite un Reporte, con las conclusiones de la restauración.

##### **CORREOS**

- ❑ El Coordinador de Sistemas, mensualmente verifica el Backup realizado mediante un servidor de desarrollo
- ❑ El Coordinador de Sistemas, verifica la idoneidad de la totalidad de los correos
- ❑ El Coordinador de Sistemas, emite un Reporte, con las conclusiones de la restauración.

##### **USUARIOS**

- ❑ El Coordinador de Sistemas, mensualmente verifica los archivos del backup con un usuario (aleatorio)
- ❑ El Coordinador de Sistemas, emite un Reporte, con las conclusiones de la restauración.

<b>Elaboración:</b>	<b>Revisión:</b>	<b>Aprobación:</b>
Diego Centeno Auxiliar de Sistemas Fecha: 13/10/2016	Rossana Delgado Coordinador del SGI Fecha: 14/10/2016	Percy Napurí Gerente General Fecha: 17/10/2016
<b>Prohibido imprimir, fotocopiar o reproducir este Documento</b>		