**CONTROL INTERNO**

**Controles Generales Organizativos**

Asegurar el correcto funcionamiento de los controles generales con las herramientas de las TI, priorizando la información para garantizar la confidencialidad, integridad y disponibilidad de la información.

**SUBCONTROL: Plan General de Seguridad.**

**RIESGOS**

1.- Incumplimiento de las normas por parte del personal.

2.- Que no se logren los objetivos planteados.

**PREVENTIVO**

1.- Condicionar a aquel que no cumpla con las normas.

2.- Darle seguimiento semanalmente a las metas que se tienen para lograr los objetivos.

**DETECTIVO**

1.- Cuando se reciban las quejas de algún cliente.

2.- Reportes de incumplimiento por parte de los empleados.

**CORRECTIVO**

1.- Sancionar al personal que ha incidentado la situación.

2.- Dar incentivos como recompensas para el cumplimiento de los objetivos.

**Controles de adquisición de sistemas de información.**

Se asegurará que las características del sistema sean las óptimas para el desenvolvimiento de las operaciones de la empresa, sin modificar el procesamiento de datos.

**Subcontrol: Explotación y mantenimiento.**

**RIESGOS**

1.- Que las características del sistema no sean las adecuadas para las necesidades.

**PREVENTIVO**

1.- Que se verifiquen las características del sistema antes de adquirirlo.

**DETECTIVO**

1.- Cuando se requiera utilizar un proceso que el sistema no contenga.

**CORRECTIVO**

1.- Generar el proceso manualmente.

**Controles de mantenimiento de sistemas de información.**

Se mantendrá el sistema de información con las características óptimas de la realización de los procesos que lleva la empresa en el tratado de datos e información.

**Subcontrol: Explotación y mantenimiento.**

**RIESGOS**

1.- Que se pospongan las fechas de mantenimiento del sistema.

2.- Que se haga un mal movimiento en el proceso de mantenimiento.

**PREVENTIVO**

1.- Programar el calendario de visitas para el mantenimiento del sistema.

2.- Conociendo el procedimiento de un mantenimiento.

**DETECTIVO**

1.- Cuando el sistema se esté saturando de información.

2.- Cuando después del mantenimiento alguna función no se haga de la misma manera.

**CORRECTIVO**

1.- Prolongar el tiempo de realización del mantenimiento.

2.- Volviendo a hacer el mantenimiento, restaurándolo a la versión anterior.

**Controles de explotación de sistemas de información**

Se revisará el estado de la computadora y se verificará que se le esté dando un buen uso a la misma para que la implementación sea exitosa sin necesidad de implementar una nueva para el sistema.

**SUB-CONTROLES**

**1.-Mantenimiento preventivo del material.**

**2.-Gestión de problemas y cambios.**

**3.-Programación del personal.**

**RIESGOS**

1.- Que el equipo de cómputo no funcione correctamente.

2.- Que no se cuente con una conexión a internet al encender la computadora.

**PREVENTIVO**

2.- Revisar el estado de la máquina constantemente.

3.- Verificar que se cuente con una conexión a internet estable.

**DETECTIVO**

1.- Revisar el problema por el cual la PC no sirve correctamente al encenderla.

2.- Revisar que el modem esté bien instalado.

**CORRECTIVO**

1.- Realizarle un mantenimiento correctivo al pc y buscar mejorar ciertas piezas de la computadora para que tenga un mejor desempeño.

2.-Revisar el modem y reportarlo en caso de estar defectuoso para su posterior cambio.

**Controles en aplicaciones**

Para la validez de los datos, cada aplicación tendrá que ser observada cada cierto tiempo, con el fin de eficientar la gestión de los datos de las aplicaciones, llevando el control de la entrada, tratamientos y salida de los datos.

**SUBCONTROL: Control de entrada de datos.**

**RIESGOS**

1.- Que el software necesite actualizarse y el espacio de almacenamiento no sea el requerido.

2.- Que surja un fallo en el hardware de la PC.

**PREVENTIVO**

1.- Vaciar parcialmente el almacenamiento de los datos que ya no se requieran.

2.- Dar mantenimiento constante a la PC.

**DETECTIVO**

1.- Cuando el software muestre una ventana del requerimiento de almacenamiento.

2.- Si la PC deja de encender o que no funcione con normalidad.

**CORRECTIVO**

1.- Cambiar el componente de almacenamiento mientras se realiza la limpieza del anterior.

2.- Asistir a un centro de reparación para conocer el fallo y la causa.

**Controles específicos de ciertas tecnologías.**

Se generará una base de datos para resguardar los datos de la empresa, esto para que siempre estén dentro de un servidor en la web para que no corran riesgos de perdida de los mismos, así como una red que sea segura y permita compartir datos entre los hosts.

**SUB-CONTROLES**

**1.-Controles de seguridad lógica.**

**2.-Monitorización para medir la eficiencia de la red.**

**3.-Existencia de inventario de todos los activos de la red.**

**RIESGOS**

1.-Que la conexión entre host y Servidor se pierda durante el guardado de datos.

2.-El servicio de internet sea deficiente a la hora de implementar el sistema.

3.-Se de un mal uso a la red cuando los empleados estén usando la computadora.

**PREVENTIVO**

1.-Restringir ciertas características de la red.

2.-Dejar de saturar la red.

3.-Hacer un listado de que puede hacer el usuario en la red.

**DETECTIVO**

1.-Revisar si hay ping entre hosts.

2.-Revisar que los cables estén bien conectados.

3.-Revisar el ancho de banda.

**CORRECTIVO**

1.-Proponer que inviertan en un servicio más eficiente de internet y comenzar a diseñar nueva topología.

2.-Listar los sitios a los que puede acceder el usuario dentro de la red y diseñar nuevamente las restricciones de red.

3.-Restringir los usuarios que tienen acceso a la red y dar permisos a los que administren él sistema.