**Propuesta de control interno.**

***Controles generales organizativos.***

En base a nuestras políticas establecidas en el manual de la organización, se hara uso del control organizativo para verificar que se este cumpliendo con lo establecido en dicho documento referente a la administración y gestión empresarial.

***Controles de explotación de sistemas.***

En base a las políticas de utilización del sistema de información que se va a implementar, vamos a verificar y velar por el buen uso de este, asi como de la neutralidad de los datos y seguridad de los mismos.

**Asignación y uso de recursos**

1.- El personal que se encarga de ventas, inventario y compras, tiene asignado un equipo donde se debe ingresar el usuario y su contraseña.

*(El riesgo que existe es que el personal proporcione datos de la empresa a terceros sin autorización y dichos datos sean robados)*

2.- El uso de internet solo es permitido para consultas que van con el entorno de trabajo cuando sean requeridas, se restringe con contraseña en el navegador instalado por defecto.

*(Se debe de tener un control de firewall ya que una conexión a Internet en sitios poco confiables puede llevar a la pérdida de información o la descarga de archivos maliciosos para el sistema)*

3.- El personal debe de aprovechar los recursos informáticos que se le proporcionan haciendo uso correcto de los mismos, reportar cualquier uso indebido del equipo, o fallas con el área de soporte.

*(Si el personal al no reporta algún defecto con el sistema se pone en riesgo toda la información almacenada o alteración de la misma)*

***Controles de aplicación.***

Nos vamos a basar en la verificación y validación de las políticas de seguridad de los datos establecidas en el manual de organización de la empresa, con el objetivo de comprobar la integridad y el tratamiento de los datos ingresados y salientes del sistema.

**Seguridad de la información**

1.- Se realizan respaldos de información automáticos a la base de datos según los parámetros establecidos y se realizaran cada 12 horas.

*(Por seguridad ante algún error en el hardware se debe de tener una copia de los datos en la nube o en otro dispositivo de confianza en caso de robo o algún daño causado)*

2.- Las sesiones de Windows estarán protegidas por usuarios y contraseñas diferentes para cada uno.

*(Todo el contenido Cómo contraseñas o datos de importancia deben de estar cifrados ante una divulgación de sus datos del empleado)*

3.- Los usuarios deberán abstenerse de compartir o divulgar sus datos de acceso a los programas y usuarios de Windows.

*(El riesgo es que un usuario se confíe o apunte en algún papel o nota sus datos de acceso, de forma que es información personal debe de evitar perder esos datos)*

4.- En todos los equipos se realizará un escaneo para verificar que no existan virus en ellos por lo menos cada mes.

5.- Todos los equipos tendrán deshabilitados los accesos a puertos USB, CD o Diskettes.

*(El riesgo es que algún usuario rehabilite dichos puertos)*

6.- Los usuarios deberán informar de manera inmediata si se encuentra algún problema de seguridad, tal como el robo de información, el cambio de contraseñas de los usuarios de Windows, existencia de algún virus o similar.

*(El riesgo es que olviden hacer dichos reportes)*

***Controles específicos de tecnología.***

Se va a verificar la integridad de la base de datos, la estructuración de las redes (topologías lógicas y físicas) y el buen uso del sistema en general. Esto en base a las políticas informáticas establecidas en el manual de organización.

**Sobre el mantenimiento y buen uso de la infraestructura**

1.- Todos los equipos deberán tener las últimas actualizaciones de Windows, así como los correspondientes parches de antivirus y seguridad adicional.

*(El riesgo es que puedan olvidar actualizar el software)*

2.- Todo el equipo informático perteneciente a la microempresa, es para uso exclusivo de actividades referentes a esta, por lo tanto, los usuarios no deberán hacer uso de estos para asuntos personales a menos que exista una autorización previa.

*(El riesgo está en que el personal puede que haga caso omiso a la política establecida)*

3.- Los usuarios no podrán instalar software de terceros sin autorización previa.

*(El riesgo es que los usuarios hagan caso omiso a la política establecida e instalen software sin autorización)*

4.- Para cada mantenimiento a la versión del software, se deberá tener un registro y un respaldo de la información, así como su debida documentación.

*(El riesgo es que se olviden los mantenimientos y/o su documentación)*