1.2.3. Políticas de seguridad .

A continuación se presentan un conjunto de actuaciones a llevar a cabo como parte de la política de seguridad. Estas actuaciones no son todas las que se pueden llevar a cabo, pero no por sencillas u obvias, no dejan de ser absolutamente necesario plasmarlas específicamente en documentos para que quede constancia y poder después efectuar las sanciones pertinentes ante posibles quebrantos de la seguridad. Son:

- Control de acceso físico a terminales y Pcs mediante llaves, candados o cualquier procedimiento que una vez forzados delaten una manipulación del sistema.
- Revisar el trafico entrante en la intranet. Todo tráfico del que no pueda determinarse su origen será cancelado.
- Tener habilitada la autenticación de usuarios.
- Definir y categorizar la información para establecer qué nivel de protección llevar a cabo.
- Revisar periódicamente los puntos críticos y obtener los parches que proporcionan para el sistema los suministradores con los que se trabaja.
- Asegurarse que todos los puntos críticos, servicios, ordenadores etc, están siendo monitorizados y restituidos ante fallos. Se

deberá guardar la información de las configuraciones existentes en un lugar de máxima seguridad.

- Desarrollar pruebas periódicas de integridad y buen funcionamiento del sistema de protección.
- Tener habilitadas las herramientas de encriptación para cifrar/descifrar datos.
- Suprimir todos los nombres de usuario, cuentas, correos etc, del personal de la empresa que deje de pertenecer a ella.
- Definir un procedimiento que informe desde el área de Recursos Humanos al gestor del sistema cada vez que se produzca una baja en la empresa.
- Especificar los pasos a acometer por parte del personal ante la caída del sistema o un funcionamiento anómalo del mismo.
- Informar a los empleados de lo que se espera de ellos para con lo que a la seguridad del sistema se refiere, de la transmisión y protección de documentos y en general de lo que pueden o no hacer. Esto supone una redacción clara y concisa por parte de un equipo de directivos, abogados, personal informático del sistema y usuarios de la intranet en un escrito que se difundirá por los distintos departamentos.
- Revisión de la política una vez lleve funcionando un plazo de tiempo determinado para detectar posibles fallos o circunstancias que afecten directa o indirectamente el buen funcionamiento de la

empresa.

- Revisión anual de la política seguida, o en periodos menores de tiempo si así lo aconseja el personal cualificado para ello.

Todo ello, llevará a una configuración, que por lo menos teóricamente, está controlada y se conoce cómo actuar en cada momento, permitiendo ejercer lo que para la empresa es su misión fundamental, el comercio.