Seguridad:

1. Física:
	* Luz solar.
	* Suelo estable.
	* Poco tráfico humano.
	* Alarma y bloqueo de sistema.
* Redes:
	+ Asegurar red física.
	+ Seguridad del sistema físico y de red.
	+ Tráfico de la red aprobado.
	+ Tráfico de red no aprobado.
	+ Desarrollo de creación y mantenimiento de cuentas de los usuarios.
1. Usuario:
	* Limitación de los recursos.
	* Limitación en la conexión a la red.
	* Registros de actividad.
	* Revisión periódica.
2. Administración del sistema:
	* Control de tamaño y ubicación de los archivos.
	* Ejecución de herramientas craaking.
	* Comprobar la vulnerabilidad del sistema de forma manual.
	* Mantener a los usuarios informados sobre las modificaciones y la seguridad.
3. Almacenamiento de Datos de Seguridad:
	* Reconocimiento de los diferentes niveles de protección.
	* Estructura general de los sistemas de archivo.
	* Restricción de acceso.
	* Revisión de seguridad de los protocolos.
	* Copias de seguridad.
	* Base de datos solo accesible para usuarios autorizados.
4. Protocolo y Servicios:
	* Actualización de software de seguridad.
	* Reconocimiento de los nuevos softwares.
	* Comprobar configuración de instalación de software.
	* Almacenamiento seguro.
	* Controlar la sobrecarga del sistema.
	* Reconocimiento de programas y almacenamiento.
	* Seguimiento de los patrones típicos de software.