1.5.2 Técnicas

El trabajo cubrirá los siguientes aspectos técnicos:

- Técnicas y sistemas de backup y recuperación.
- Métodos de archivado.
- Integridad de bases de datos.
- Autentificación de los usuarios.
- Criptografía.
- Firewal de la intranet de la F.A.N.
- Gestión de contraseñas.
- Estadísticas de gestión de integridad y seguridad.
- Documentación y manejo de procedimientos.

1.5.3 Administrativas:

El trabajo se limitará y desarrollará en los Componentes del Ejército y la Armada venezolana, con la finalidad de crear un modelo de gestión de seguridad e integridad, que fácilmente sea parametrizable para las otros Componentes de la F.A.N.

Otras limitaciones estarán constituidas por la información de tipo confidencial que se genera y procesa en la organización seleccionada, por su naturaleza y rol estratégico en la Nación.

1.5.4 Supuestos Implícitos.

- Autenticidad y veracidad de los documentos utilizados para diseñar la arquitectura de la seguridad de la información para la F.A.N.
- Necesidad de la F.A.N., en la propuesta de seguridad y sus políticas de los medios electrónicos.
- La validez del método y de las herramientas a utilizar para el diseño en el ámbito técnico.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo esta basado en tecnología moderna, para esto se debe conocer que la información:

- Está almacenada y procesada en computadoras.
- Puede ser confidencial para algunas personas o a escala institucional.
- Puede ser mal utilizada o divulgada.
- Puede estar sujeta a robos, sabotaje o fraudes.

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que hoy se sufre un accidente en el centro de computo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Para continuar es muy importante conocer el significado de dos palabras, que son riesgo y seguridad.

Riesgo : Proximidad o posibilidad de un daño, peligro, etc.

Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Seguridad: Cualidad o estado de seguro.

Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Ejemplo: Seguridad Social, conjunto de organismos, medios, medidas, etc., de la administración estatal para prevenir o remediar los posibles riesgos, problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del Estado, trabajadores y empresarios.

Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Con estos conceptos claros podemos avanzar y hablar, la criminología ya ha calificado los "delitos hechos mediante computadora o por "sistemas de información" en el grupo de delitos de cuello blanco.

Seguridad en Internet

Hoy en día, muchos usuarios no confían en la seguridad del Internet. En 1996, IDC Research realizó una encuesta en donde el 90% de los usuarios expresó gran interés sobre la seguridad del Internet, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la Red.

Ellos temen que otros descubran su código de acceso de la cuenta del banco y entonces transferir fondos a la cuenta del hurtador. Las agencias de gobierno y los bancos tienen gran preocupación en dar información confidencial a personas no autorizadas. Las corporaciones también se preocupan en dar información a los empleados, quienes no están autorizados al acceso de esa información o quien trata de curiosear sobre una persona o empleado. Las organizaciones se preocupan que sus competidores tengan conocimiento sobre información patentada que pueda dañarlos.

Aunque los consumidores tienden a agrupar sus intereses juntos por debajo del término de la seguridad general, hay realmente varias partes de la seguridad que confunden. La Seguridad significa guardar "algo seguro". "Algo" puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactiva. "Seguro" los medios son protegidos desde el acceso, el uso o alteración no autorizada.

Para guardar objetos seguros, es necesario lo siguiente: