

TUTORIAL DE PROTECCION DE LAS INFORMACIONES MEDIDAS DE CONTRAINTELIGENCIA

Se establece una oficina segura, protegida contra todo tipo de espionaje moderno, garantizando el manejo de las informaciones, minimizando los riesgos de ser visto y/o escuchado y/o grabado desde el interior o desde el exterior, inclusive por visitas y/o personal dependiente que tenga acceso al objetivo.

Se pretende brindar protección física, en las comunicaciones y en el archivo de voz, datos e imágenes.

El propósito es proteger:

1. Contra escuchas o filmaciones ambientales, realizadas en una oficina internas y/o externas y/o observaciones encubiertas.
2. Contra captura y monitoreo de datos Informáticos.
3. Conversaciones telefónicas desde teléfonos fijos, móviles y portátiles.
4. Contra grabaciones no autorizadas.

La protección se brinda mediante la utilización de equipos que permiten la detección y/o bloqueo de la acción no deseada. La verdadera seguridad de las Informaciones, es decir las Contramedidas Electrónicas parten del criterio de que la seguridad debe ser redundante y por lo tanto como no se sabe con que medios ni que recursos utilizara el oponente es que debe buscarse la excelencia tratando siempre de implementar el nivel mas alto posible de protección conjuntamente con la redundancia de los sistemas.



Detección.

1. Alto nivel de seguridad. Implica medidas activas y pasivas tales como la instalación de:
 - Analizadores de espectro de banda corrida.
 - Pórtico detector de metales.
 - Detectores de líneas instalados en redes de alimentación eléctrica y de datos.
2. Nivel de seguridad medio
 - Detectores Fijos y/o Portátiles
 - Pórtico detector de Metales
3. Bajo nivel de seguridad.



Consiste en la mínima protección a instrumentarse mediante sistema detección portable en el propio cuerpo o también con Detectores Portátiles que se pueden trasladar de un ambiente a otro (no tienen la misma eficacia de los que están instalados en forma fija).



Bloqueo.

En el bloqueo los niveles de Seguridad son:

1. Alto nivel de bloqueo. Implica la instalación de láminas en las paredes, pisos y techos que producen una jaula de faraday casi perfecta, impidiendo la circulación de señales de cualquier tipo
2. Nivel medio. Generadores de Ruidos ambientales audibles
3. Bajo Nivel. Conformado exclusivamente por Jammers que bloquean parcialmente algunos equipos electrónicos tales como Micrófonos Inalámbricos, o Celulares, o teléfonos inalámbricos.

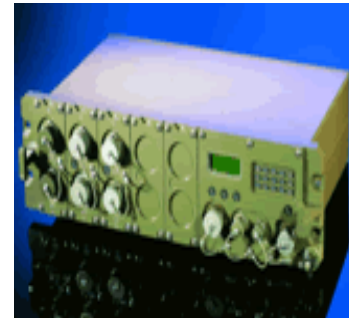


SISTEMAS DE CRIPTOGRAFIA

Nixon comercializa en Argentina, los sistemas criptográficos Hagelin, empresa número uno en seguridad de Información en más de 130 países en todo el mundo.

La Comunicación de Hoy requiere disponibilidad de información alrededor del mundo las 24 hs y enfrenta tres amenazas básicas:

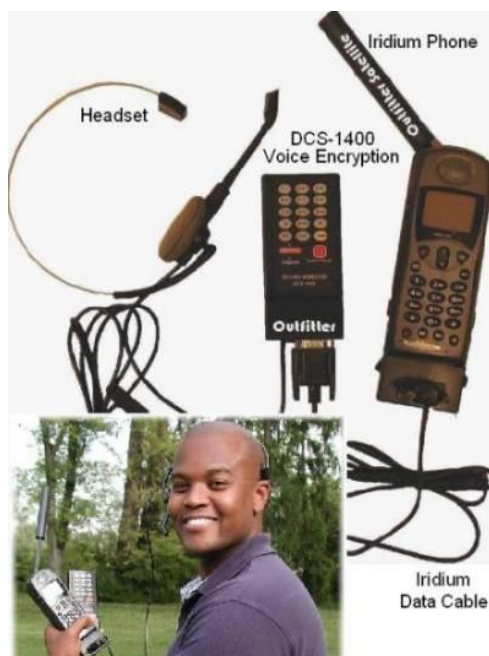
- Pérdida de confiabilidad: lectura de la información o escucha.
- Pérdida de la integridad: modificación o eliminación de la información.
- Pérdida de autenticación: enmascaramiento, falsificación.



TELEFONOS SATELITALES CRYPTO

Permiten estar comunicados en cualquier lugar del mundo en voz y datos, en forma flexible, confiable y segura. Cobertura Universal al 100 %

- Un solo número de teléfono en todo el mundo.
- Sistemas de Paging y Voz.
- Teléfonos portables y livianos
- El kit incluye panel solar, módem para conexión de notebook, notebook crypto, maletín de transporte, antenas para vehículos, aviones y barcos.



COMUNICACIONES CLASIFICADAS

Todas las comunicaciones de voz que, por este medio, realicen entre sí los integrantes del grupo de conversación, dentro del ámbito de la República Argentina serán sin cargos adicionales de comunicación por todo el tiempo que las mismas se extiendan y estarán protegidas por una VPN (cifrado opcional).

Todos los integrantes de esta Red pueden realizar en forma ilimitada sus comunicaciones de voz mediante una Red Privada Virtual (VPN), exclusivamente entre sí y con alcance Nacional.

Todos los equipos de esta Red Cerrada, están bloqueados a fin de evitar que se realicen comunicaciones (entrantes y salientes) con otros equipos fuera de la Red.

Se utilizará una denominación "no llamativa" de la red (para no ponerla en evidencia).

Llamada en espera: Permite recibir, durante la comunicación en curso, un aviso en el terminal que indicará la existencia de una segunda llamada. Se podrá retener la primer llamada mientras se atiende la segunda y alternar entre ambas y/o realizar multi conferencias.

Identificador de llamadas:

TELEFONOS CELULARES CRYPTO

Comunicaciones telefónicas seguras, dentro de una Red Privada Virtual, con alta calidad de audio y baja latencia. Evita que la información confidencial pueda llegar a las manos equivocadas.

El sistema de encriptación utilizado es de alta seguridad, empleando una doble capa de algoritmos, con claves de encriptación automáticamente generadas por el teléfono y sin utilizar servidores externos.

Cuando un usuario desea iniciar una comunicación segura, simplemente debe presionar la tecla C del teléfono lo que inicia la sesión encriptada. Luego insertará el número deseado en la pantalla correspondiente (o lo elige desde la agenda del terminal) y presionará SEND. Si el número al que llama pertenece a un terminal con igual sistema de encriptación, igual versión de software y dentro de la misma VPN, la comunicación se realizará en forma "protegida" (modo Seguro). En caso contrario, no podrá realizar la comunicación "segura".

Si bien la interface de usuario es muy simple, la tecnología involucrada es realmente sofisticada.

El software interviene encriptando voz y texto por medio de una formulación matemática de doble capa que crea una clave asimétrica de 1024 bits basada en el algoritmo RSA y una clave de sesión dinámica de 256 bits que modifica la encriptación cada segundo. El intercambio de claves se asegura con Diffie Hellman de 4096 bits.

Características Generales:

- No depende de un servidor externo.



- Sin puertas traseras - las llaves de encriptación son generadas en forma aleatoria por el software.
- Protección total punto a punto, de teléfono a teléfono, para audio y mensajes de texto.
- Combinación dual de encriptación asimétrica y simétrica.
- Baja latencia.
- Excelente calidad de audio.
- Par de llaves maestras asimétricas RSA de 1024 bits..
- Algoritmo simétrico AES de 256 bits para protección de datos.
- Algoritmo Diffie-Hellman con llave de 4,096 bits para intercambio seguro de claves.
- Clave maestra aleatoria de 1024 bits generada por contacto y reemplazada con cada comunicación.
- Llave de sesión aleatoria de 256 bits reemplazada cada segundo.



TELEFONIA SATELITAL IRIDIUM

Para naves fluviales-marítimas

Aplicaciones para diferentes usos, incluyendo el uso comercial para personas que deben estar en contacto con sus oficinas localizadas en otros continentes, servicio para naciones en desarrollo sin una intranet.

Sólo NIXON IRIDIUM pone en la palma de su mano la comunicación global satelital, otorgándole la conveniencia de una comunicación portátil y la capacidad para que cuide de su negocio sin importar donde usted se encuentre.



Para Aeronaves

Su oficina en el cielo:

- Helicópteros
- Jets
- Kit para tripulantes.
- Kit para pasajeros.

