



ARMADA ARGENTINA • SERVICIO DE CIBERDEFENSA Y SEGURIDAD DE LA INFORMACION





ARMADA ARGENTINA • SERVICIO DE CIBERDEFENSA Y SEGURIDAD DE LA INFORMACION



CIBERDEFENSA Y SEGURIDAD EN LAS COMUNICACIONES



TEMARIO

CIBERESPACIO

CIBERDEFENSA

CONCEPTOS SOBRE SEGURIDAD DE LAS COMUNICACIONES

ARQUITECTURA DE SEGURIDAD DE LAS COMUNICACIONES

CRIPTO SISTEMAS - CONSIDERACIONES GENERALES

MODELO DE SEGURIDAD DE LAS COMUNICACIONES



CIBERESPACIO

Ámbito operacional virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y explotación de información digital, a través de redes interdependientes e interconectadas, vinculadas a internet o no y el software y firmware de dispositivos asociados a las mismas, siendo su carácter distintivo el empleo excluyente de las TICs (Tecnologías de Información y Comunicaciones) y la interacción permanente con los otros ámbitos operacionales.

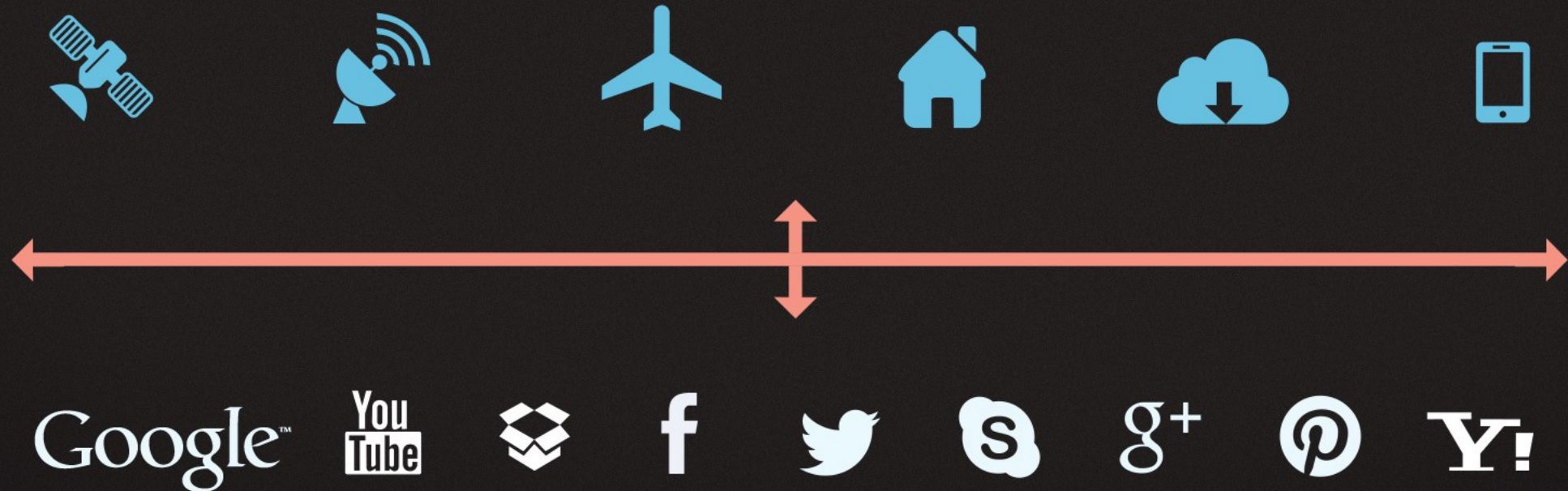


CIBERESPACIO – INFRAESTRUCTURA





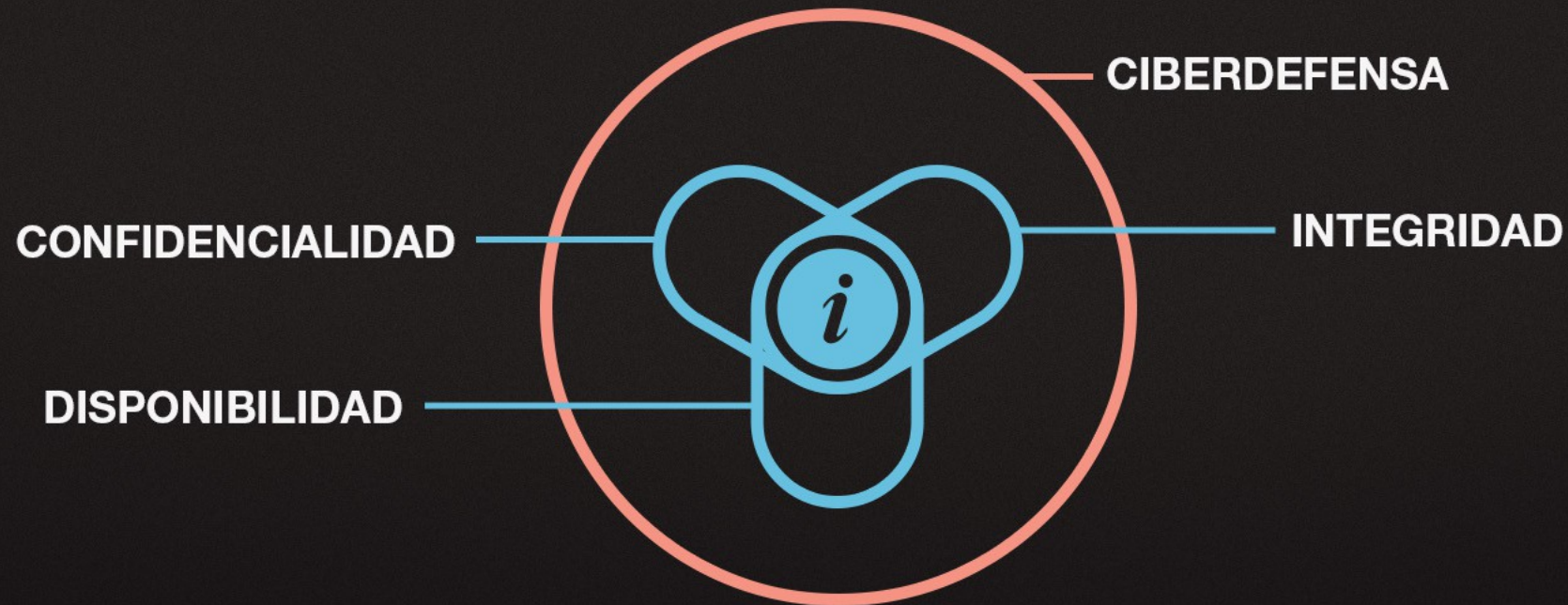
CIBERESPACIO - ACCESO - MANEJO





CIBERDEFENSA

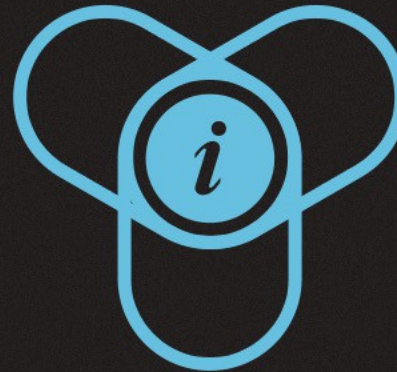
La Ciberdefensa debe estar dirigida a combatir o contrarrestar una amenaza, sea esta inmediata, latente o potencial, originada en adversarios, enemigos, organizaciones criminales o individuos aislados, que pretenda atentar contra los principios de Confidencialidad, Integridad y Disponibilidad de la Información, debiéndose considerarse como una función defensiva-ofensiva.





CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

LAS COMUNICACIONES SIN IMPORTAR
EL VINCULO UTILIZADO SON INTERCEPTABLES



INTERCEPCIÓN, ANÁLISIS DE TRÁFICO,
CRIPTOANÁLISIS, CAPTACIÓN DE
EMISIONES ELECTROMAGNÉTICAS ESPURIAS

OBTENER , ALTERAR O PERTURBAR
LA INFORMACIÓN O SU TRANSMISIÓN



CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

CLASIFICACION DE REDES DE COMUNICACIÓN POR SU CONDICION DE SEGURIDAD

- REDES NO CONTROLADAS
- REDES CONTROLADAS
- REDES EN AMBITO PROTEGIDO



CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

REDES NO CONTROLADAS :

COMUNICACIONES QUE AL MENOS EN UN TRAMO CIRCULAN FUERA DE JURISDICCIÓN PROPIA.





CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

REDES CONTROLADAS :

COMUNICACIÓN POR CABLE, JURISDICCIÓN PROPIA, ADMINISTRADA, MANTENIDA, CONTROLADA Y OPERADA POR PERSONAL PROPIO

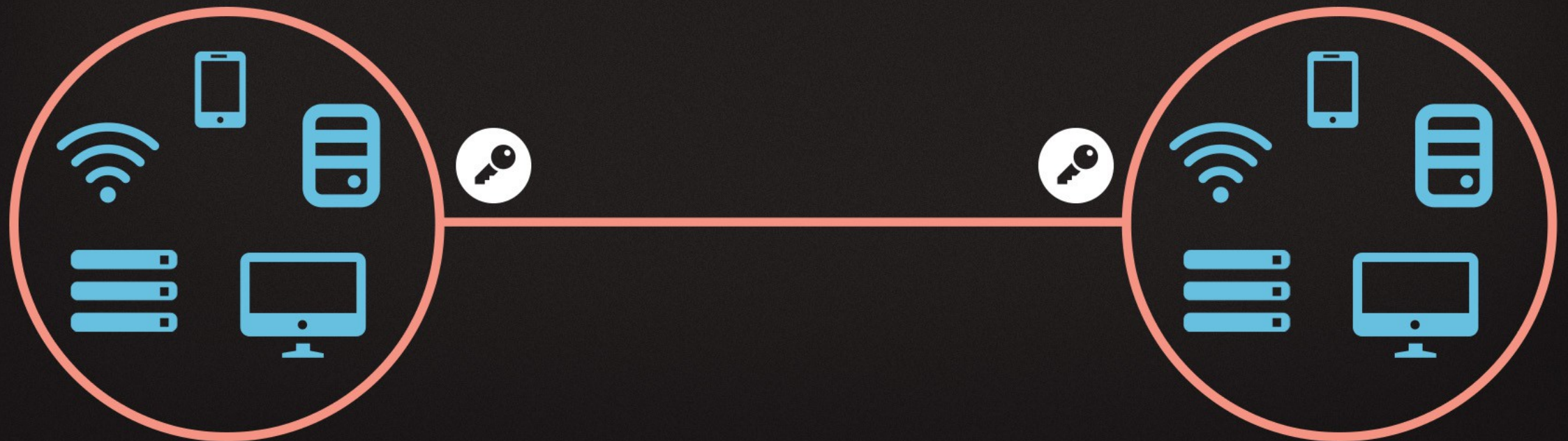




CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

AMBITO PROTEGIDO

REDES CONTROLADAS CON VINCULO PROTEGIDO CRIPTOGRAFICAMENTE

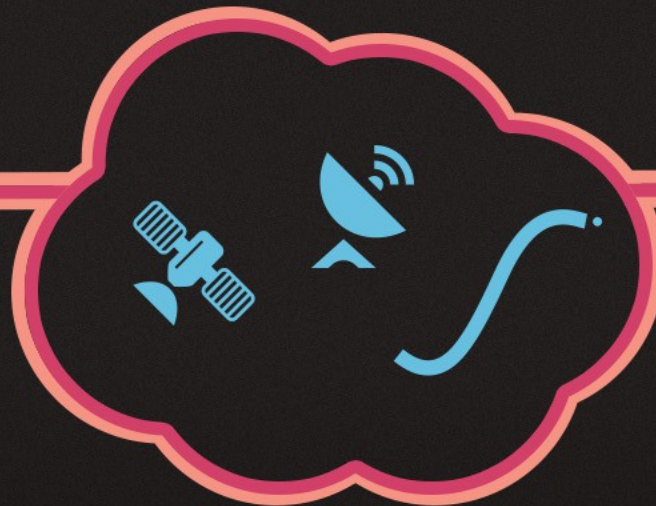




CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

TRANSMISION DE INFORMACION SEGÚN LA CONDICION DE SEGURIDAD DE LAS REDES

REDES NO CONTROLADAS



TODO EL TRÁFICO CIFRADO
(P - R - C)
Y SECRETO PUNTO A PUNTO





CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

TRANSMISION DE INFORMACION SEGÚN LA CONDICION DE SEGURIDAD DE LAS REDES

REDES CONTROLADAS



TODO EL TRÁFICO CIFRADO
SECRETO PUNTO A PUNTO



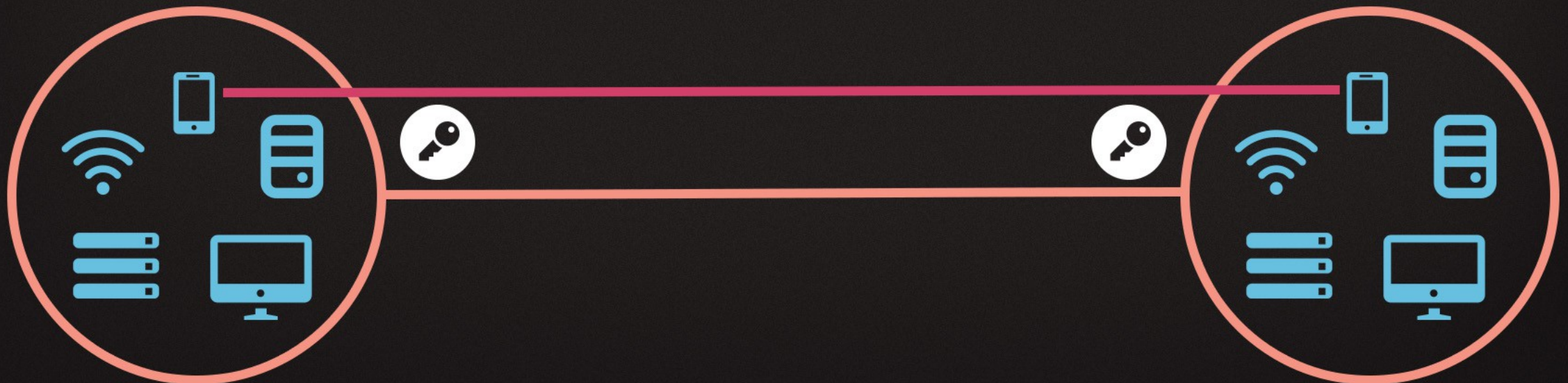


CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - CONCEPTOS BASICOS

TRANSMISION DE INFORMACION SEGÚN LA CONDICION DE SEGURIDAD DE LAS REDES

ÁMBITO PROTEGIDO

TODO EL TRÁFICO CIFRADO
SECRETO PUNTO A PUNTO





CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - ARQUITECTURA





CIBERDEFENSA - CRIPTOSISTEMAS - CONSIDERACIONES GENERALES

CONJUNTO DE ELEMENTOS CRIPTOGRAFICOS, RELACIONADOS ENTRE SI, PARA POSIBILITAR EL CIFRADO Y DESCIFRADO DE LA INFORMACION.

UN CRIPTOSISTEMA ESTARA COMPUESTO POR EL EQUIPO Y EL ALGORITMO CRIPTOGRAFICO, LA DOCTRINA QUE PERMITE SU USO Y LAS CORRESPONDIENTES CLAVES.



CONSIDERAR ACTORES CON CAPACIDAD DE :

- INTERCEPTAR LA TOTALIDAD DEL TRÁFICO
- DETECTAR ERRORES CRIPTOGRÁFICOS EN LA APLICACIÓN DE LA DOCTRINA U OPERACIÓN DE LOS CRIPTOSISTEMAS
- CRIPTOANÁLISIS Y DECISIÓN DE AFRONTAR EL COSTO DE SU UTILIZACIÓN
- DESARROLLAR SU ACCIONAR EN TIEMPO DE PAZ O GUERRA
- EMPLEAR CUALQUIER PROCEDIMIENTO PARA OBTENCIÓN DE NUESTRAS CLAVES Y/O EQUIPOS CRIPTOGRÁFICOS
- EFECTUAR EL SALVAMENTO DE LOS CRIPTOSISTEMAS DEFICIENTEMENTE DESTRUIDOS O HUNDIDOS



CIBERDEFENSA - CRIPTOSISTEMAS - CONSIDERACIONES GENERALES



CRITERIOS/RECOMENDACIONES DE SELECCIÓN DEL SISTEMA

- ENCRIPCIÓN POR HARDWARE.
- ENCRIPCIÓN SIMÉTRICA.
- CIFRADO POR BLOQUES (NO MENORES DE 128 BITS)
- LONGITUD DE CLAVE (NO MENOR A 128 BITS)
- POSIBILIDAD DE VERIFICACIÓN DEL ALGORITMO DE CIFRADO.
- POSIBILIDAD DE PERSONALIZACIÓN DEL ALGORITMO DE CIFRADO.
- CAPACIDAD DE MANEJO DE CLAVES MÚLTIPLES.
- CAPACIDAD DE GENERACIÓN DE DOMINIOS DE CIFRADO.
- ADMINISTRACIÓN DE CLAVES DE ACUERDO A ISO 11770-1-2-3
- CERTIFICACIÓN NORMA FIPS-140-2 NIVEL 4



CIBERDEFENSA - CRIPTOSISTEMAS - CONSIDERACIONES GENERALES



CRITERIOS/RECOMENDACIONES RESPECTO AL ALGORITMO DE CIFRADO

- CONOCIDOS EL CLARO Y EL CIFRADO, RESULTE IMPOSIBLE EN TIEMPO UTIL DEDUCIR EL ALGORITMO.
- CONOCIDOS EL CIFRADO Y EL ALGORITMO, RESULTE IMPOSIBLE EN TIEMPO UTIL DEDUCIR EL CLARO.
- CONOCIDOS EL CLARO, EL CIFRADO Y EL ALGORITMO, RESULTE IMPOSIBLE EN TIEMPO ÚTIL DEDUCIR LA CLAVE.
- NO GENEREN MENSAJES HOMOLOGOS .
- POSEER UNA LONGITUD DE CLAVE TAL QUE UN SISTEMA INFORMÁTICO NO SEA CAPAZ EN TIEMPO ÚTIL, DE ROMPER EL SISTEMA POR FUERZA BRUTA.
- UTILICEN CLAVES QUE HAYAN SUPERADO LOS TEST CORRESPONDIENTES.



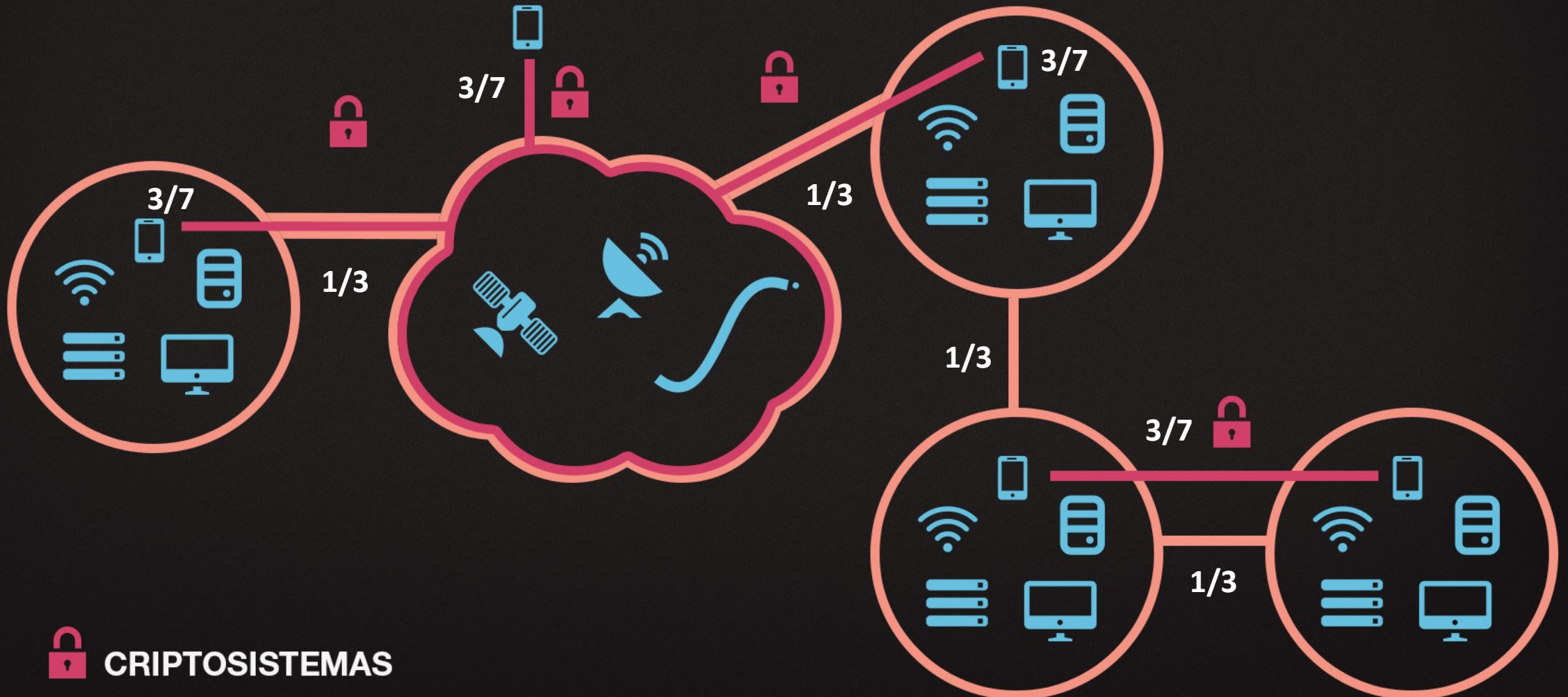
CIBERDEFENSA - MODELO DE SEGURIDAD DE LAS COMUNICACIONES

MODELO DE ENCRIPCIÓN MULTICAPA





CIBERDEFENSA - SEGURIDAD DE LAS COMUNICACIONES - ARQUITECTURA





CIBERDEFENSA - MODELO DE SEGURIDAD DE LAS COMUNICACIONES

PROTECCIÓN DE REDES

FÍSICA

LÓGICA

PROCEDIMIENTOS

AUDITORIA



DETECCIÓN Y ANULACIÓN
DE VULNERABILIDADES



Realizado por
Mano Mediaworks
manomw.com