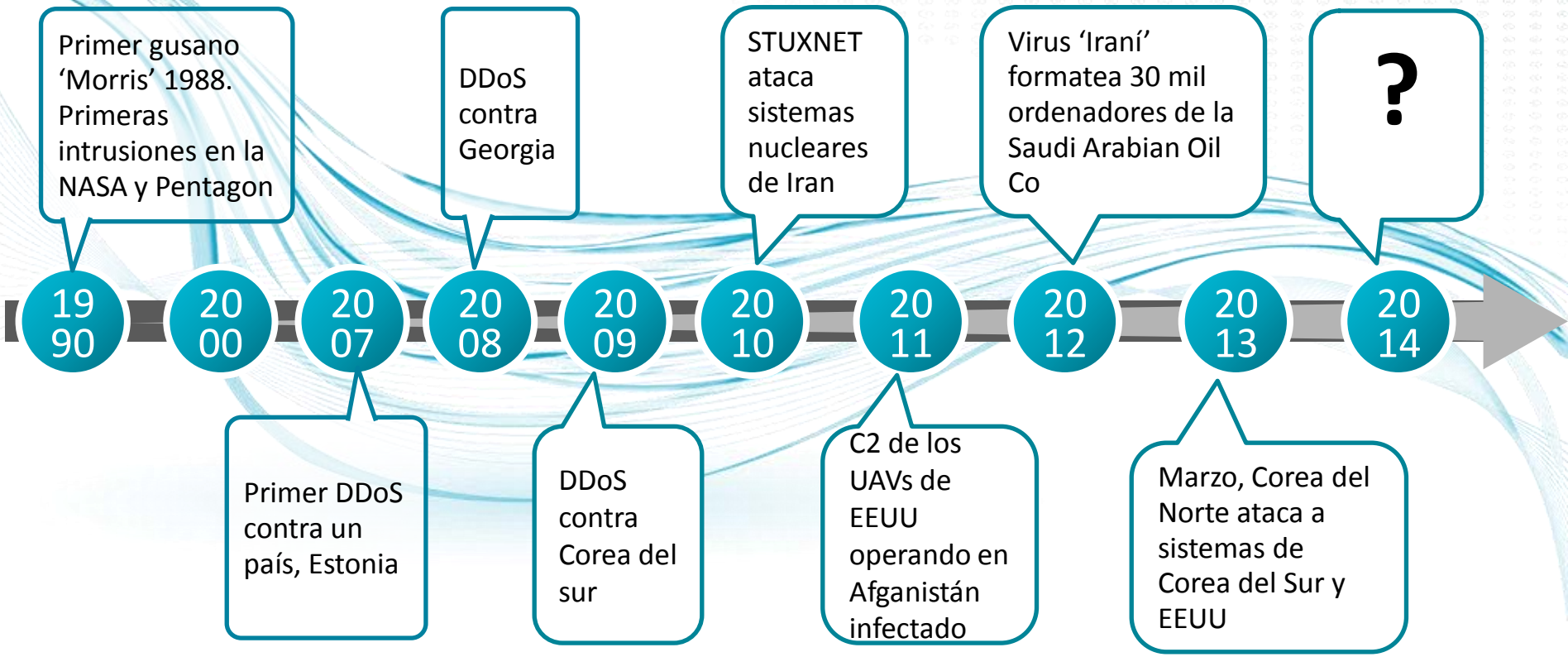
Semana Naval de la Armada

Jornadas Tecnológicas, 24 y 25 septiembre 2013

Ciberdefensa: Retos y Oportunidades para el Sector de la Defensa y Seguridad

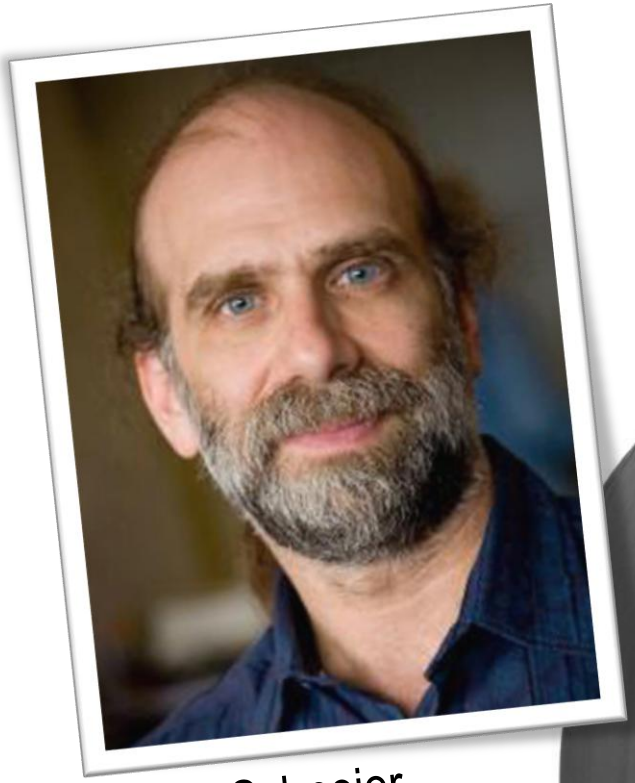
indra

UN PASO ADELANTE: CRONOLOGÍA DE LOS CIBERATAQUES



FAMILIARIZARSE CON LA NORMALIDAD

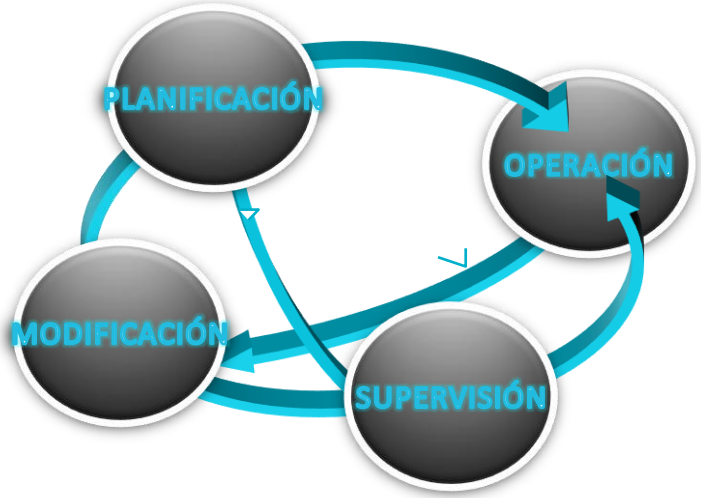
"En el ciberespacio, el balance de poder está en el lado del atacante. Atacar una red es más facil que defenderla…"



Bruce Schneier
Schneier on Security

SINGULARIDADES

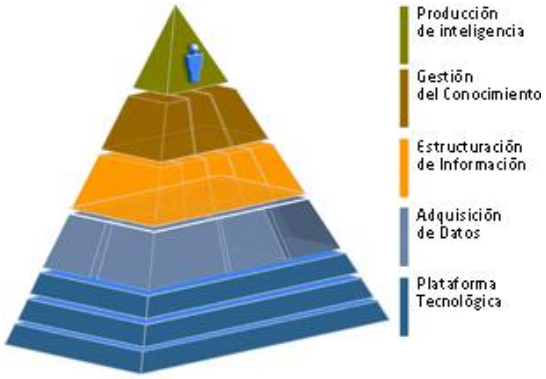
- El medio ya no es sólo físico, sino virtual y no sólo natural sino también artificial
- La amenaza no es sólo cinética y tangible, sino también cibernética e intangible
- No existe el concepto clásico de fronteras y límites de influencia
- No existen barreras de distancia ni temporales
- La velocidad de desarrollo de acontecimientos se ha acelerado hasta el límite de haber alcanzado otro orden de magnitud



CONCIENCIA SITUACIONAL

La Ciberinteligencia y Conciencia Situacional son claves para conocer el estado de seguridad de las redes e identificar y predecir las amenazas cibernéticas

CIBERINTELIGENCIA y ALERTA TEMPRANA



La ciberinteligencia ofrece mejor calidad de información para facilitar la toma de las mejores decisiones:

- Tratamiento, clasificación y pre-análisis de información mediante un equipo de analistas
- Identificación temprana de ciberamenazas, análisis posterior y comunicación eficaz a los usuarios
- Uso de la información sobre vulnerabilidades recopilada de las diferentes ubicaciones protegidas
- Clasificación y ponderación de la gravedad de las diferentes amenazas

CONCIENCIA SITUACIONAL

Análisis dinámico de riesgos para ofrecer una visión en tiempo real de las amenazas a las que están expuestas las ubicaciones y su evolución

Integración de varios elementos en una consola única de situación (CROP) para poder reaccionar ante amenazas cibernéticas

BIG DATA

La captura masiva de datos permite descubrir los “unknown unknowns”,
y las técnicas de big data permiten el análisis y correlación entre estos datos

El General Keith Alexander, jefe del Cibercomando Estadounidense y la NSA

EL ESTADO COMO ENEMIGO

BBC NEWS TECHNOLOGY

12 October 2012 Last updated at 10:38 GMT

US prepares first-strike

Cyber-attacks could inflict as much damage on the US as the physical attacks on 11 September 2001, the US defence secretary has warned.

Leon Panetta said the country was preparing to take pre-emptive action if a serious cyber-attack was imminent.

The New York Times

Panetta Warns of Dire Threat

By ELISABETH BUMILLER and THOM SHANKER

Published: October 11, 2012

Defense Secretary Leon E. Panetta warned Thur
States was facing the possibility of a "cyber-Pear
increasingly vulnerable to foreign computer hac
dismantle the nation's power grid, transportatio
networks and government.

REUTERS

Exclusive: Insiders suspe
cyber attack

By Jim Finkle

Fri Sep 7, 2012 4:52am EDT

(Reuters) - One or more insiders with high-level access are suspected of assisting the hackers who damaged some 30,000 computers at Saudi Arabia's national oil company last month, sources familiar with the company's investigation say.

website hacked by Syria's Assad loyalists

Tue, Sep 4 2012

Exclusive: White House studying potential oil reserve

CNN

EL PAIS

INTERNACIONAL

Estados Unidos y China, ante la primera ciberguerra fría

Obama firmó una orden ejecutiva la pasada semana que le otorga poderes especiales

ANTONIO CAÑO | Washington | 19 FEB 2013 - 20:06 CET 135

Archivado en: Barack Obama Guerra electrónica Ataques informáticos China Ciberactivismo Seguridad internet Asia oriental Activismo Guerra Estados Unidos Internet Norteamérica Asia Telecomunicaciones Conflictos América Comunicaciones

El presidente Barack Obama durante una intervención en Washington este martes. / JIM LO SCALZO (EFE)

La Casa Blanca describió este martes los reiterados ataques cibernéticos, que una investigación reciente vincula directamente con una unidad secreta del Ejército chino, como "un serio desafío para la seguridad y la economía de Estados Unidos", lo que es la señal de que una nueva guerra fría, en el desconocido e incontrolable espacio de Internet, ha comenzado entre las dos grandes potencias que se disputan la supremacía en el siglo XXI.

Sin acusar directamente a China, por

Algunos comentaristas se asombraron cuando, hace poco menos de un año, un alto funcionario del Ministerio de Defensa de Estonia, Mijaíl Tammet, le dijo a la BBC que ambas situaciones eran comparables.

Chertoff instó al sector privado a colaborar con el gobierno.

EL PAIS Internacional

Nacional Internacional España Deportes Economía Tecnología Cultura Gente y TV Sociedad Opinión Blogs Participa

América Latina | Europa | Estados Unidos | Oriente Próximo | Corresponsales

ENTREVISTA DIGITAL ¿Dónde invertir en Bolsa? Pregunta EN DIRECTO al experto de Atlas Capital Ignacio Cantos

nformático afecta a 30.000 ordenadores

leares está a salvo del gusano Stuxnet

están a salvo, pero ha reconocido que adores dentro de su territorio y continúa deojuego, se trata de algo mucho más a no operaba correctamente por unos programas troyanos

sta de los 'ciberataques' jército chino revela una la que pocos esconden

dificio de la 'Unidad 61398'. | Foto: City8.com, via Mandiant

iro Mejía (Efe) | Washington

tualizado jueves 21/02/2013 10:11 horas

Comentarios

revelación de identidades y 'modus operandi' de los miembros de la puesta unidad de 'hacking' más secreta del Ejército chino ha sido talladas hasta el extremo y los expertos consideran que China

INTERNET EN LOS DISPOSITIVOS: BYOD

La “internetización” de los dispositivos informáticos, tanto personales como embebidos en nuestro entorno, implica un punto de entrada para atacantes y un riesgo para la confidencialidad

EVALUACIÓN DEL RIESGO: SISTEMAS DE "MISION COMPLETION"

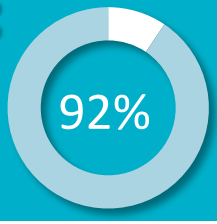
La probabilidad de ataques está aumentando

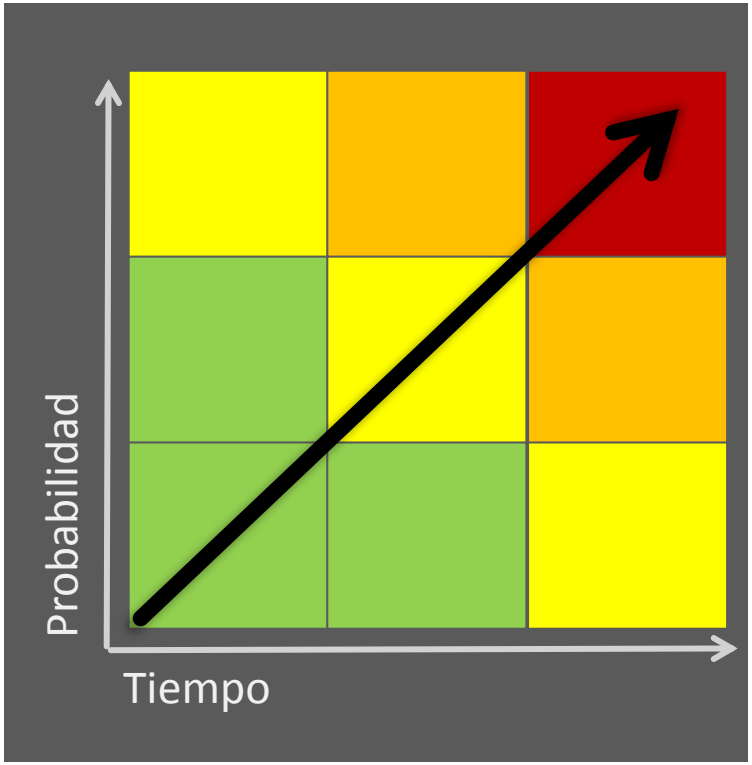
PROBA-BILIDAD EN AUMENTO

ALTO IMPACTO

Empresas atacadas

Empresas con presencia en Internet





CAMBIOS EN LA DOCTRINA MILITAR

By Jim Wolf
WASHINGTON | Tue Feb 2, 2010 3:46am IST

Feb 1 (Reuters) - The U.S. Defense Department is putting cyberspace on a par with land, sea, air and space as a potential conflict zone, and developing new ways to operate there, a top-level Pentagon's strategy review said Monday.

Operaciones en los nuevos escenarios:

- Contramedidas Defensivas no Intrusivas
- Operaciones Defensivas con efecto cibernético
- Operaciones Ofensivas con efecto cibernético

Gobiernos y organizaciones internacionales han creado cibercomandos específicos para defenderse ante las amenazas emergentes

CIBERDEFENSA ACTIVA

Métodos Pasivos

- Sistemas auto reconfigurables
- Predicción, detección
- Mitigación
- Métodos de intercambio de información

Métodos Activos

- Ataques anticipados
- Atribución
- Sistemas de Cibercombate

El uso de sistemas de respuesta activa para la ciberdefensa está en sus primeros pasos

LAS CIBERARMAS

ABC.es | TECNOLOGÍA

ACTUALIDAD DEPORTES CULTURA VIAJAR GENTE&ESTILO TV VIDEO SALUD BLOGS

España Internacional Economía Sociedad Bodas Toros Madrid Ediciones Ciencia Medios Familia Defensa Opinión

TECNOLOGÍA / CIBERGUERRA

Descubren la mayor «ciberarma» de la historia del espionaje en internet

El virus Flame llevaba operativo 5 años en Oriente Medio, por lo que otras armas similares pueden estar ya en funcionamiento

J. F. A. / MADRID

Día 29/05/2012 - 09.16h

```
assert(loadstring(config.get("LUA.LIBS.table_ext")))()
if not __LIB_FLAME_PROPS_LOADED__ then
    LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSI
    flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTER
    flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.B
    flame_props BPS_KEY = "BPS"
    flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERV
    flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
            local l_1_0 = config.get
            local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
            return l_1_0(l_1_1)
```

ABC

Imagen de Flame, un virus malicioso utilizado como arma cibernética

http://www.bbc.co.uk/news/ News | Sport | We

BBC Mobile

NEWS 20 September 2011 Last updated at 10:56 GMT

Home UK Africa Asia-Pac Europe Latin America Mid-East South Asia US & Canad

Magazine In Pictures Also in the News Editors' Blog Have Your Say World Radio a

LATEST: China denies suggestions it may have been responsible for hacking attack on Jap

Japan defence hit by cyber attack

Japan's biggest weapons maker laur investigation into a cyber attack, bel first of its kind against the country's industry

E-mail hack attacks an 'epidemic'

Cyber-attack hits Lockheed Martin

Cyber-sabotage tops security fear

Italy has debt rating cut by S&P

Italy's credit rating is cut by Standard and Poor's, but Prime Min Berlusconi says the move is based on "political considerations".

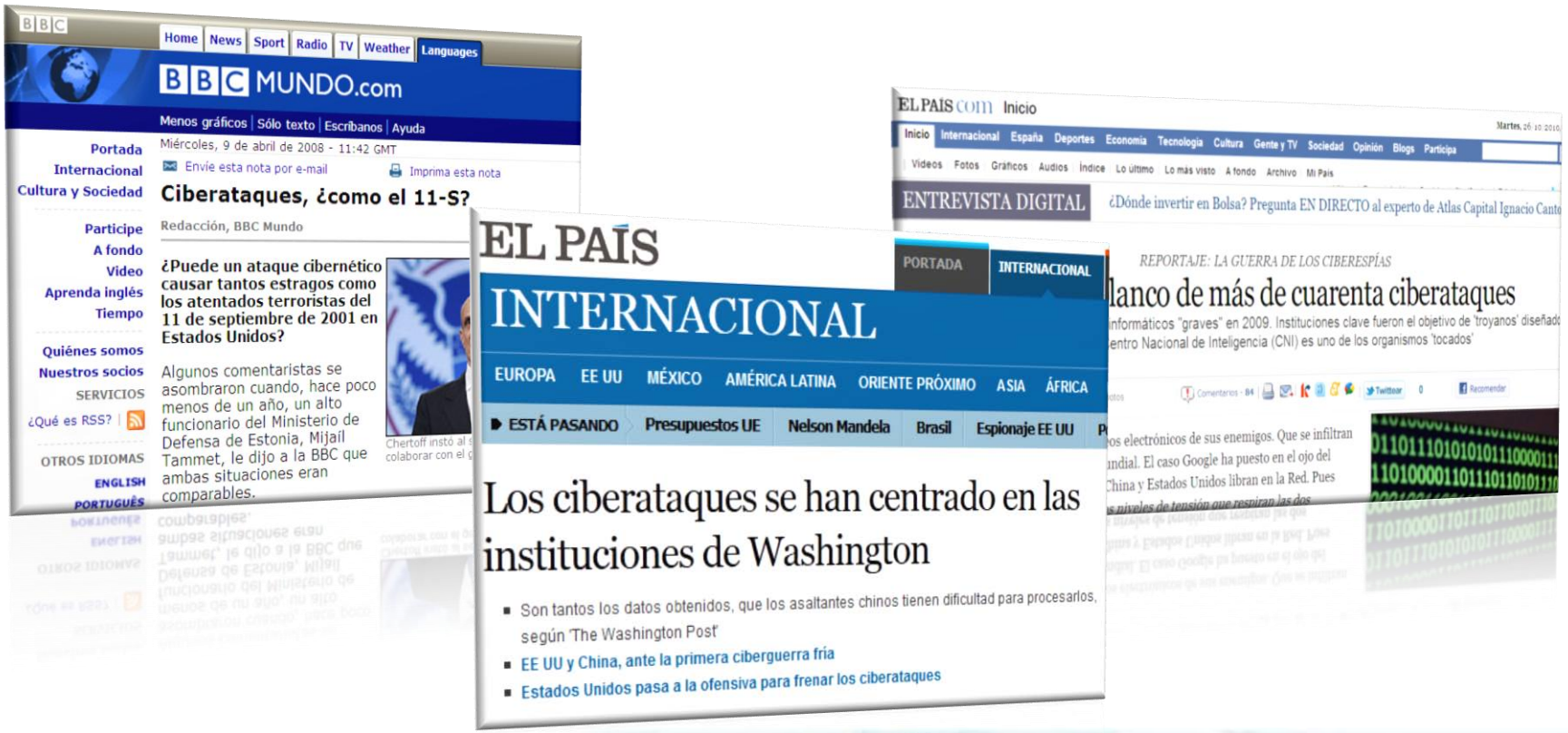
Greece bailout talks 'productive' In graphics: Deficits c

LOS PARADIGMAS ESTÁN CAMBIANDO

El incremento de la dependencia de los Sistemas de Información

La complejidad de los medios TIC: Cloud Computing

Ciberguerra como una amenaza real



FORMACIÓN Y ENTRENAMIENTO EN CIBERDEFENSA

La formación en técnicas de Ciberdefensa es imprescindible para tener una capacidad efectiva

Prevención
análisis de vulnerabilidades, configuración segura, gestión de parcheo

Detección y reacción
configuración segura de redes y sistemas; monitorización y gestión de la seguridad (SIEM, Firewall, IDS/IPS, network probing, …)

Análisis forense
análisis de disco duro y memoria de S.O. en búsqueda de evidencias; obtención y custodia centralizada de evidencias; generación de informes

Ataque
exploración e identificación de objetivos; análisis de vulnerabilidades; explotación y consolidación; exfiltración, escalada de privilegios y expansión

LAS NUEVAS OPORTUNIDADES

CIBERSEGURIDAD Y CIBERDEFENSA

En Indra entendemos

CIBERSEGURIDAD

como el conjunto de tecnologías, procesos, procedimientos y servicios encaminados a proteger los activos (físicos, lógicos, o de servicios) de una organización, que dependan en alguna medida de un soporte TIC

GRACIAS POR SU ATENCIÓN