Pasos a seguir para ser un profesional de Ciberseguridad

Alejandro Corletti Estrada
acorletti@darFe.es

Organización de la Seguridad

¿Cómo se organiza la Seguridad?

Seguridad en redes y TI (Desde la estrategia a la técnica)

Supongamos desde un enfoque **ISO-27000**, que nuestro ámbito de aplicación es:

"arquitectura y gestión de la red y TI de la empresa XXXX".

Presentaríamos un enfoque de:

a. **Valoración de riegos (Risk Assesment).**
b. **SGSI.**
c. **Controles.**
   - Política de seguridad
   - Organización de la información de seguridad
   - Administración de recursos
   - Seguridad de los recursos humanos
   - Seguridad física y del entorno
   - Administración de las comunicaciones y operaciones
   - Control de accesos
   - Adquisición de sistemas de información, desarrollo y mantenimiento
   - Administración de los incidentes de seguridad

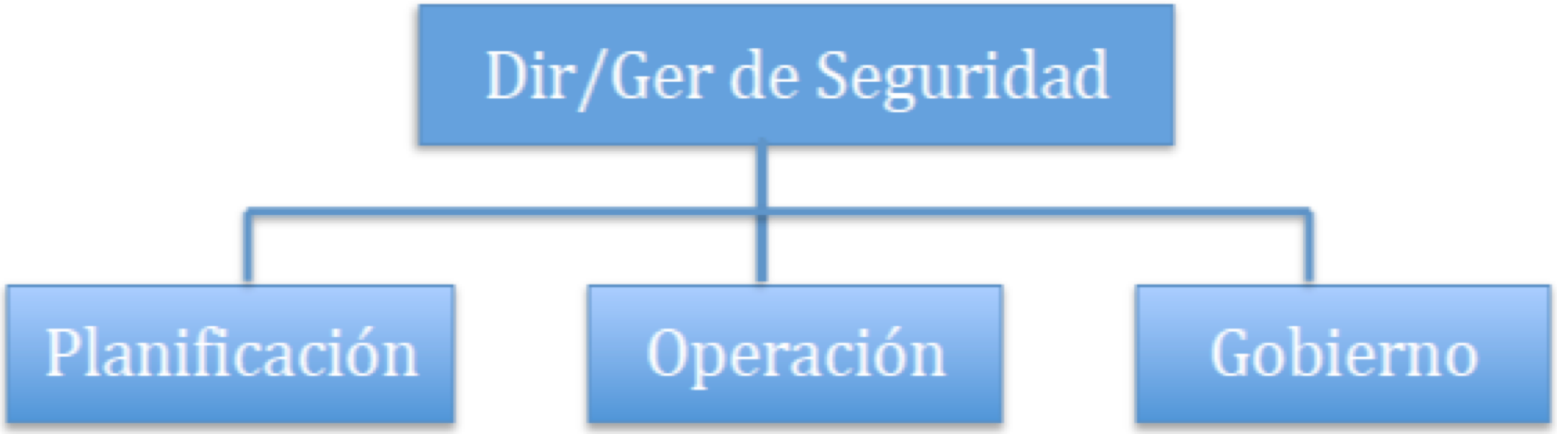
¿Cómo lo propone ISO-27000?

Áreas y funciones

www.darFE.es

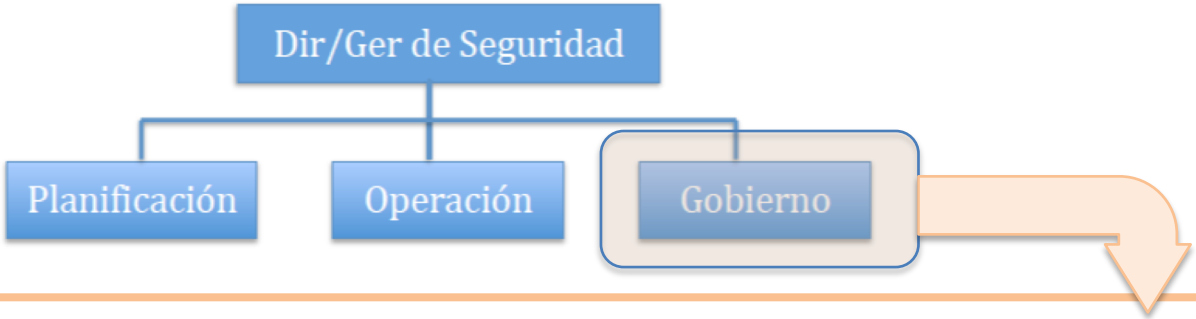
Independientemente de la magnitud de una empresa u organización debe existir un área responsable de seguridad de redes y TI.

Sea una sola persona o toda una dirección, debería desempeñar las siguientes funciones:



Gobierno de la seguridad

www.darFE.es



ISO-27000 → ámbito de aplicación: "**arquitectura y gestión de la red y TI de la empresa XX**".

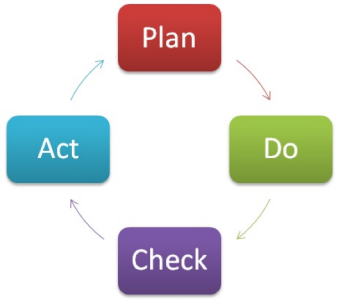
Presentaríamos un enfoque de:

a. Valoración de riegos (Risk Assesment).

b. SGSI.

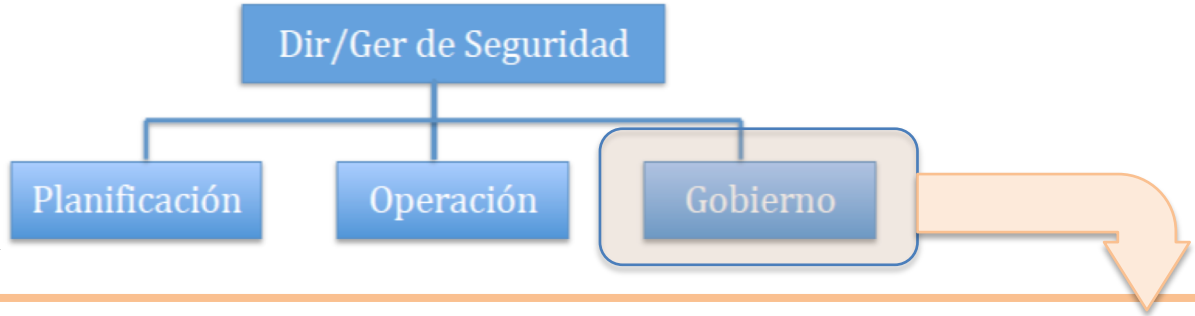
c. Controles.

1. Política de seguridad
2. Organización de la información de seguridad
3. Administración de recursos
4. Seguridad de los recursos humanos
5. Seguridad física y del entorno
6. Administración de las comunicaciones y operaciones
7. Control de accesos
8. Adquisición de sistemas de información, desarrollo y mantenimiento
9. Administración de los incidentes de seguridad
10. Administración de la continuidad de negocio
11. Marco legal y buenas prácticas



Plan Director de Seguridad

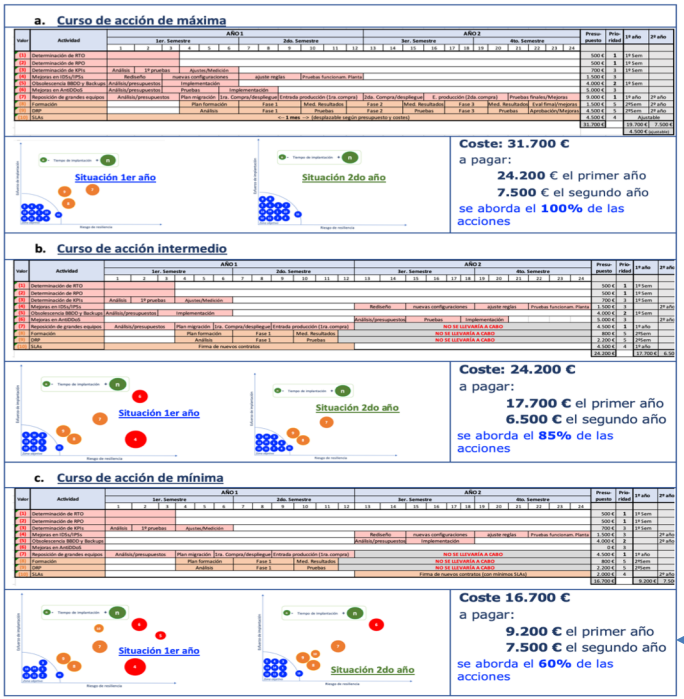
www.darFE.es



Plan Director de Seguridad

Descargar Documento: *"Plan Director de Seguridad (una visión: práctica, eficiente y estándar)"*

Las claves de un plan son: Identificar y dividir el problema → priorizar → simplificar → agendar → y supervisar...*nada más que esto*



Cursos de acción

Ilustración 1
Implantando un Plan Director de Seguridad

Según **INCIBE**:

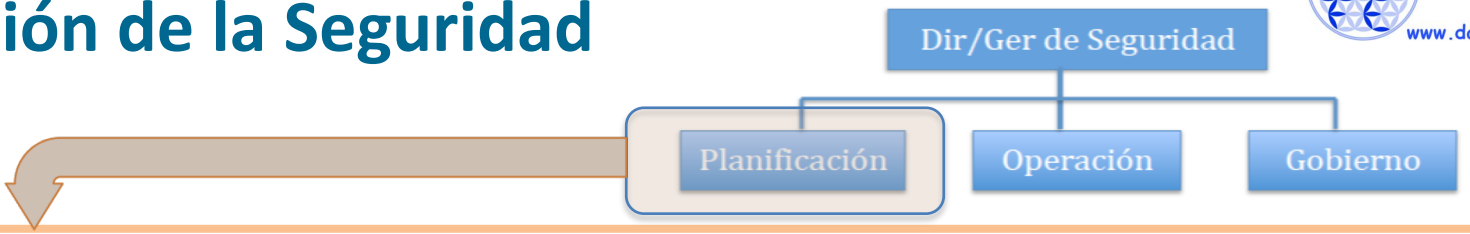
PLAN DIRECTOR DE SEGURIDAD

Consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

Riesgo:

- Recursos (Activos)
  - Inter relación entre activos
    - Valoración
      - Exposición
        - Impacto
          - Amenazas
            - Probabilidad de ocurrencia
              - Dimensiones
                - Vulnerabilidades
                - Salvaguardas
                - Cursos de acción
                - *(Decisión de la dirección)*
                - Riesgo residual

Planificación de la Seguridad



¿Qué debe hacer planificación?

a. **Análisis técnico**. (Análisis de Viabilidad Técnica):

¿Qué subprocesos contempla?

a) Especificación Técnica de Requisitos funcionales, de Seguridad y de Gestionabilidad.
b) Informe de Análisis Técnico. (funcionalidad, escalabilidad, seguridad).
c) DTS (Definición Técnica de la Solución) Red Preliminar.

b. **Pruebas de Laboratorio**.

¿Qué subprocesos contempla?

a) Autorización de FOA.
b) Doc. Integración con sus OSSs.
c) Descripción técnica de detalle.
d) Documentación de Implantación para FOA.
e) Informe de Pruebas Laboratorio.

Procesos

Creación de planta	Gestión de incidencias
Gestión de accesos	Gestión de backups
Gestión de usuarios	Gestión de Logs
Gestión de configuración/inventario	Supervisión y monitorización
Gestión de cambios	

c. **Pruebas en Red** (Realización de las pruebas con tráfico real en primera instalación).

Si todo ha sido correcto los siguientes pasos serán:

a) Autorización de Introducción en planta para Despliegue.
b) Documentación de Despliegue.
c) Informe de Acreditación de Seguridad.
d) Informe de Pruebas FOA.

Elementos fundamentales de red y TI.

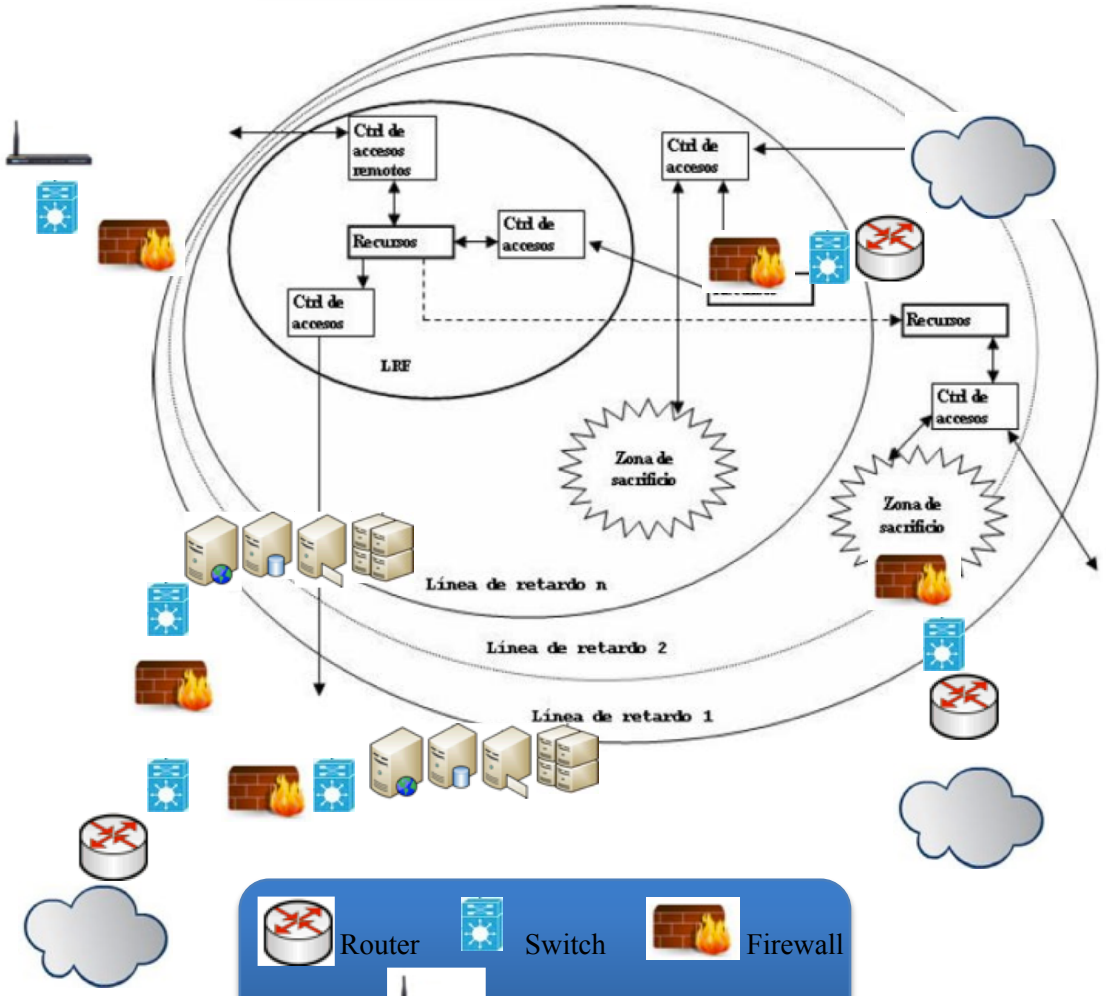
www.darFE.es

Dir/Ger de Seguridad

Planificación | Operación | Gobierno

a. Capas (Defensa en profundidad).
b. Componentes por niveles de una red.
c. Vista por niveles.

Aplicación	Usuario	Desde aquí hacia arriba mira hacia el usuario
Transporte	Es el primer nivel que ve la conexión "de Extremo a Extremo"	Desda aquí hacia abajo mira hacia la Red
Red	Rutas	
Enlace	Nodo inmediatamente Adyacente	
Físico	Aspectos Mecánicos, físicos y eléctricos (u ópticos)	



¿Qué hace cada uno de ellos?

¿Qué hace cada elemento de red y en qué nivel?

Switch (N 2) Conoce el direcc. de este nivel (**MAC**).

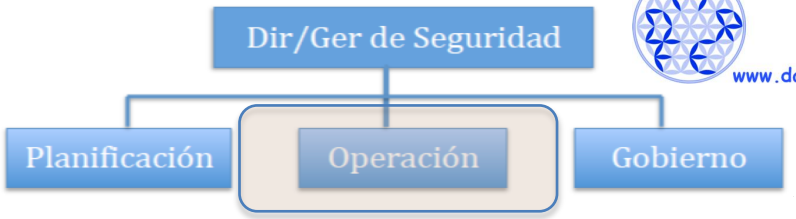
Acces Point (Nivel 2) → Conoce el direcc. de este nivel (**MAC**).

Router (nivel 3) → Conoce el direccionamiento de este nivel (**IP**).

Firewall (varios niveles) → Conoce hasta el nivel de Transporte (TCP) (*)

(*) También hay FWs de nivel Aplicación (*pero no son motivo de esta charla*).

Operación de la Seguridad



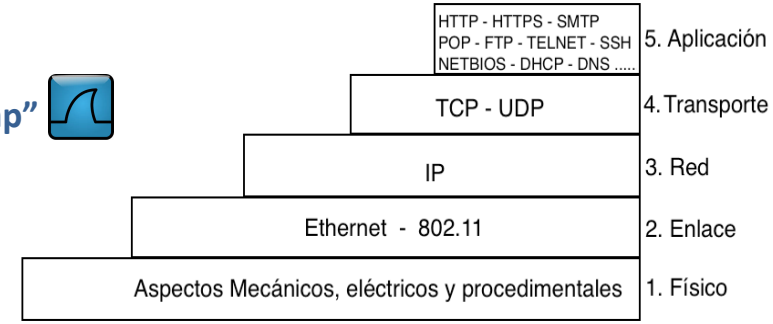
www.darFE.es

¿Qué debe hacer operación?

¿Cómo se analizan los niveles? → **"Wireshark"** (Ethereal) o **"tcpdump"**

¿Cómo analizo elementos de red? → **nmap**

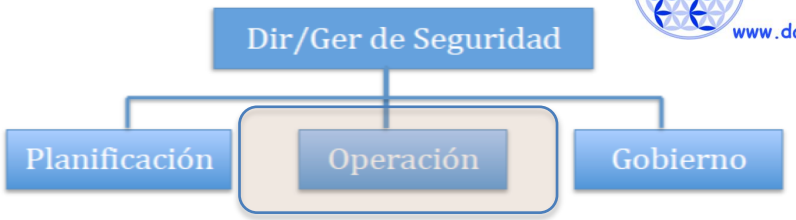
¿Cómo analizo redes WiFi? → Suite **"aircrack-ng"**: (*airodump, aireplay, aircrack-ng*)



Acciones preventivas y reactivas basadas en el empleo de lo siguiente:

- Herramientas de mitigación de ataques DDoS tipo TMS/Peak Flow de Arbor
- Herramientas de centralización y correlación de Logs (SIEM) del tipo:
  - ✓ ArcSight de HP, RSA Security Analytics, Splunk
- Firewalls. En el mercado existen cientos.
- Herramientas de gestión de Firewalls del tipo: Algosec, Tuffin, Firemon
- Herramientas de detección y prevención de intrusiones del tipo:
  - ✓ Snort, Check Point IPS, Cisco NG-IPS, McAfee NSP
- Herramientas de monitorización y supervisión de red. existen cientos.
- Herramientas de gestión de ticketing. también existen varias.
- Herramientas de control de acceso, tipo:
  - ✓ ACS Cisco, Series SRC de Juniper, NAKINA, Acc. Ctrl. Fortinet, HPNA, CITRIX
- Metodología estricta de sincronización de tiempos basada en el protocolo NTP.
- Herramientas forenses

Operación de la Seguridad



www.darFE.es

Referentes nacionales e internacionales

Guías CIS: http://www.cisecurity.org/ CIS Center for Internet Security®

Serie 800 CCN-CERT-CNI: Guías Esquema Nacional de Seguridad CCN centro criptológico nacional

NIST: NIST National Institute of Standards and Technology U.S. Department of Commerce

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER (CSRC): Publicaciones

INCIBE-CERT: Publicaciones incibe-cert_

CMMC: Modelo CMMC

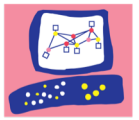
Office of the Under Secretary of Defense for Acquisition & Sustainment
Cybersecurity Maturity Model Certification

ISO27000.ES

Web iso27000.es: Resúmenes, guías y herramientas de ISO 27000

Formación en Seguridad

Formación



- Profesionales cualificados y con experiencia.
- Formación y certificación (Sun MicroSystems / Oracle, CheckPoint, Cisco, CEH (Certified Ethical Hacker), CISSP (Certified Information System Security Professional), NATO, Guidance, …)
- Estrategia ofensiva vs. defensiva.

El mundo del Hacking Ético

El HE es una excelente herramienta para calibrar con precisión los ciberriesgos:

- **Sus principales capacidades son:**
  - Auditoría a distancia de entornos complejos en cualquier ubicación.
  - Identificar e inventariar las vulnerabilidades asociadas a cada elemento de red y/o sistema.
  - Identificar los vectores de ataque más factibles y analizarlos para calibrar el riesgo real que suponen para la compañía.
  - Identificar qué activos están expuestos a internet y tomar las correspondientes evidencias.
  - Hacer un seguimiento ágil y eficiente de los planes de remediación al permitir un retesting inmediato para verificar la efectividad de las medidas correctivas adoptadas.
  - Análisis forenses detallados para calibrar el daño/alcance real de una infiltración e identificar los vectores de ataque utilizados.

- **Otras capacidades adicionales. Alerta temprana:**
  - Identificación proactiva de amenazas y ataques de Zero-Day.
  - Seguimiento, investigación e infiltración en los foros “underground” para:
    - Identificar robos de información o acciones dolosas contra la compañía.
    - Establecer mecanismos de alerta temprana para prevenir/gestionar con antelación ataques de hacktivismo.

El HE es una actividad profesional y estandarizada

A la hora de identificar las vulnerabilidades y calibrar los riesgos se aplican estándares internacionalmente reconocidos:

- **OSSTMM. Open Source Security Testing Methodology Manual.**
- Es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet.
- Incluye un marco de trabajo que describe las fases que habría de realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre cientos de expertos internacionales sobre el tema, que colaboran entre sí mediante Internet.

http://osstmm.org

- **CVSS. Common Vulnerability Scoring System.**
- Con el objetivo de valorar de forma objetiva las vulnerabilidades utilizamos la metodología CVSS que es el estándar internacional de facto.
- La elección de esta métrica se basa en la necesidad de tener un sistema de valoración independiente de los fabricantes y respaldada por un organismo de referencia a nivel mundial como el FIRST

http://first.org/cvss/

El HE es una actividad profesional y estandarizada

Para soportar nuestras recomendaciones aplicamos igualmente dos estándares internacionales:

- **OWASP. Open Web Application Security Project.**
- La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo.
- Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.
- Estar libre de presiones corporativas facilita que OWASP proporcione información imparcial, práctica y reutilizable sobre seguridad de aplicaciones informáticas.

http://owasp.org

- **CIS. Center for Internet Security.**
- Es una organización sin ánimo de lucro cuya misión principal es mejorar los niveles de ciberseguridad y la capacidad de respuesta a los ciberriesgos de las entidades públicas y privadas. Entre sus miembros se encuentra el US Departament of Homeland Security.
- Posee una de la más amplia, reputada y mejor contrastada biblioteca de guías técnicas de bastionado.

http://cissecurity.org

Futuro en Seguridad

Tendencias de futuro

www.darFE.es

Nuevos ciberriesgos emergentes de alto impacto potencial.

- **Ciberterrorismo.**
  - La conexión a la red de multitud de activos estratégicos hace cada vez más verosímil para las agencias gubernamentales de seguridad la posibilidad de sufrir un ataque ciberterrorista.

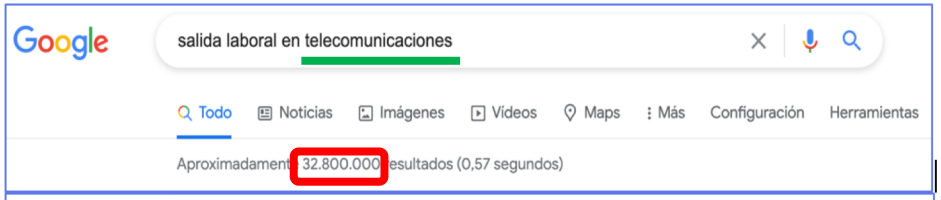
- **Ciberespionaje.**
  - Esta actividad orientada al robo de información de alto valor estratégico es muy lucrativa. La incorporación de los gobiernos a esta actividad incrementará de forma significativa los riesgos al espionaje industrial, económico, político y militar.

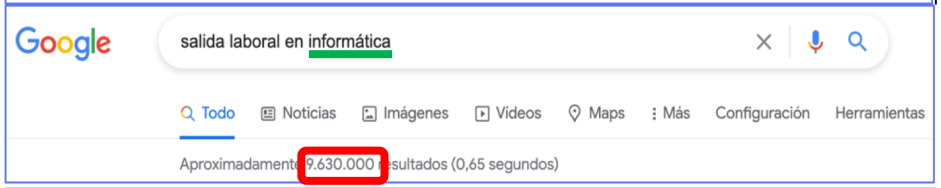
- **Ciberguerra.**
  - La OTAN en su estrategia considera el Ciberespacio como un escenario más de guerra. La aplicación del arte de la guerra, la dotación de recursos y los programas de I+D+i en ciberarmas supondrá un cambio importante en los modelos y esquemas de protección de las infraestructuras críticas.

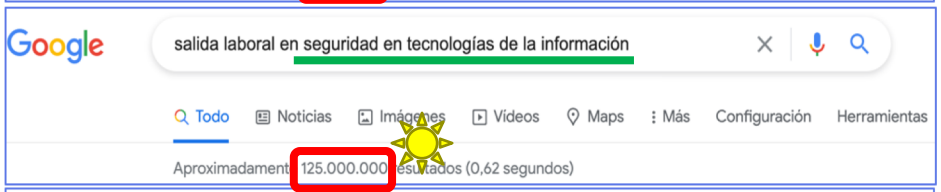
La principal particularidad de este ciberespacio "hiperconectado" es que en él se está en contacto permanente con el enemigo.

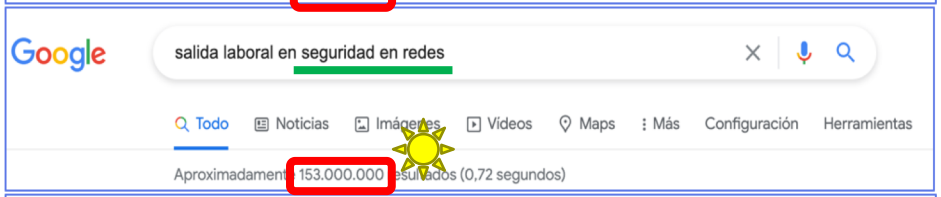
Salida laboral

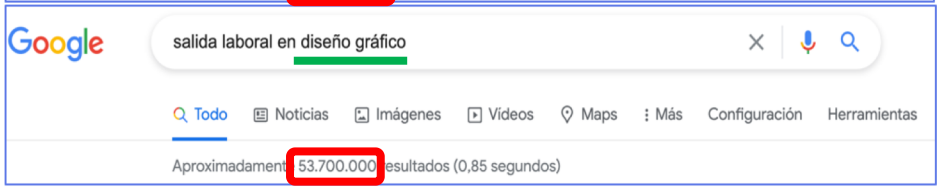
www.darFE.es

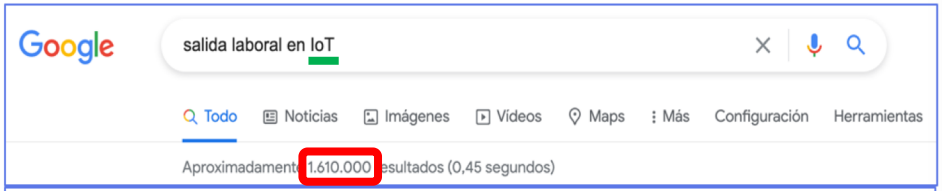


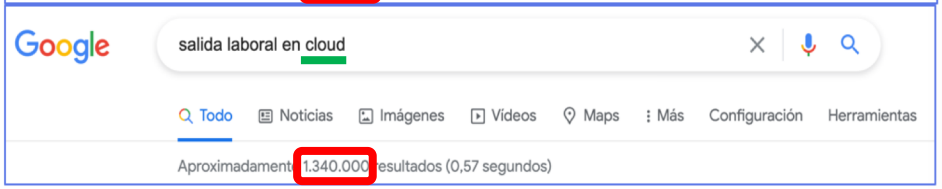


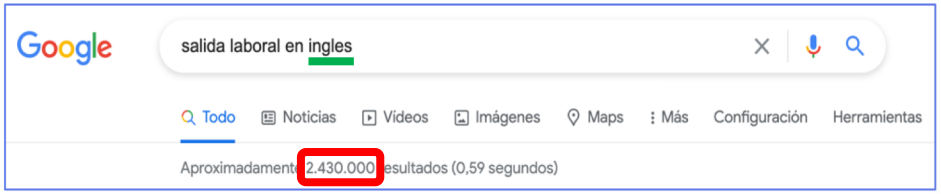


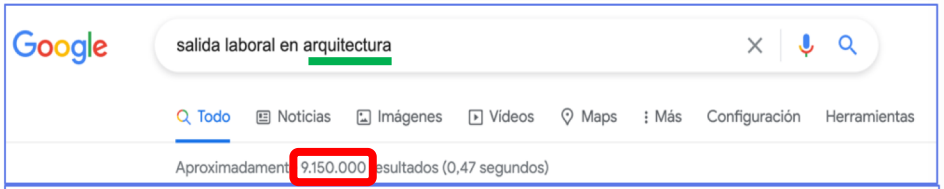


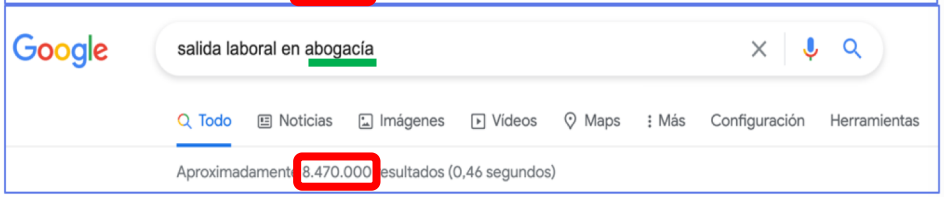












www.darFE.es

GRACIAS

Alejandro Corletti Estrada
acorletti@darFe.es