Gobierno, Planificación y Operación de la Ciberseguridad

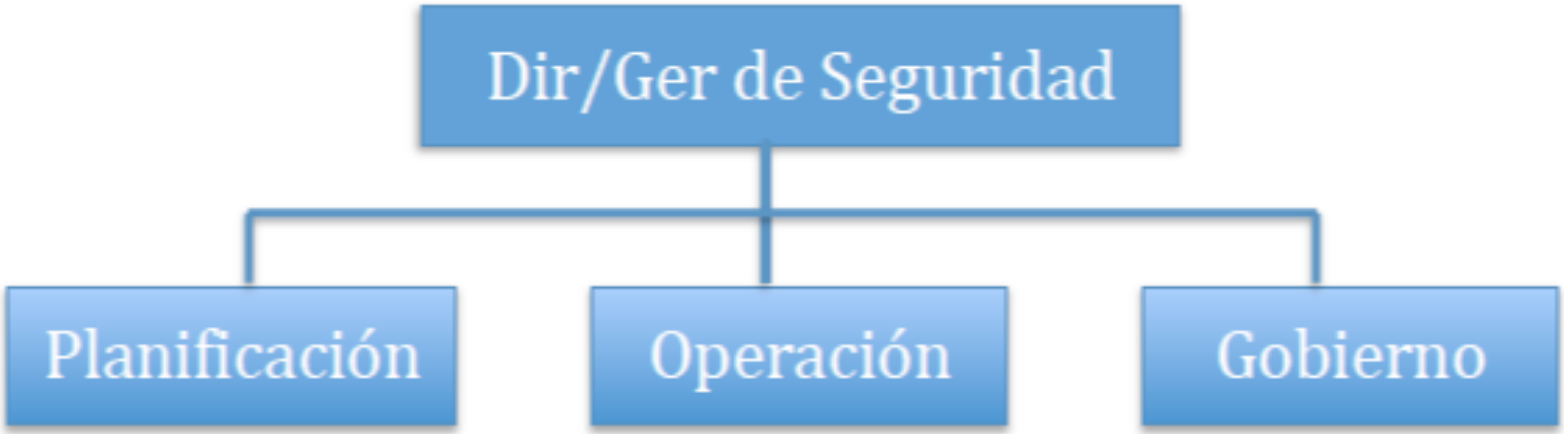
¿Y los servicios digitales financieros? (DFS)

Alejandro Corletti Estrada
acorletti@darFe.es
www.darFe.es

Organización de la Seguridad

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

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

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*

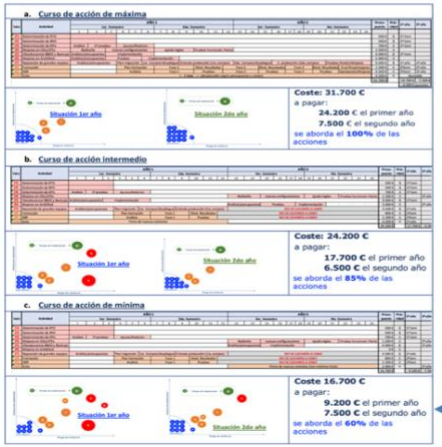


Ilustración 1
Implantando un Plan Director de Seguridad

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:

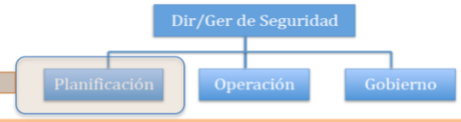
- Recursos (Activos)
  - Inter relación entre activos
    - Valoración
      - Exposición
        - Impacto
          - Amenazas
            - Probabilidad de ocurrencia
              - Dimensiones
                - Vulnerabilidades
                - Salvaguardas
                - Cursos de acción
 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

Cursos de acción

Ver detalle en el libro:
"**Manual de la Resiliencia**"

www.darFe.es

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.

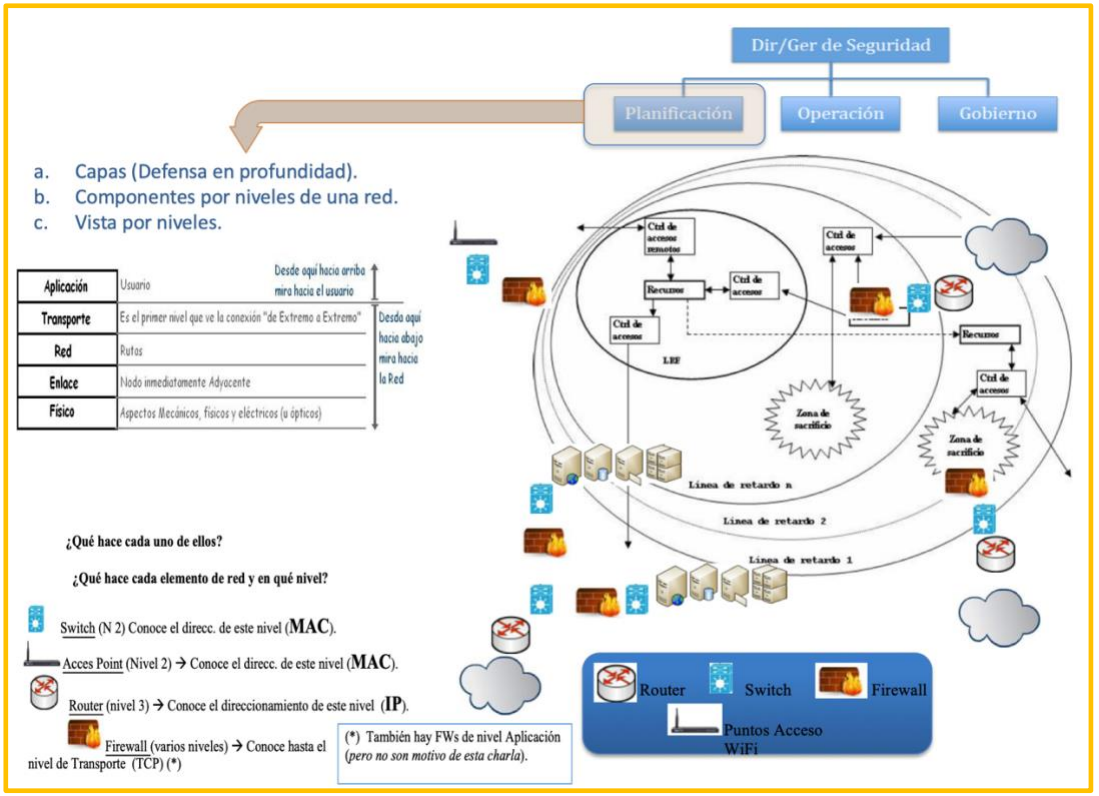
Procesos

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:

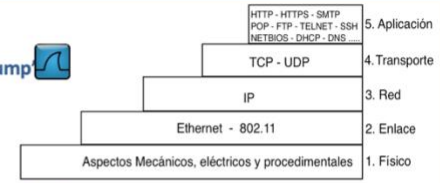
a) Autorización de Introducción en planta para Despliegue.
b) Documentación de Despliegue.
c) Informe de Acreditación de Seguridad.
d) Informe de Pruebas FOA.



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 Microfocus, 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, Data Center Automation, CITRIX
- Metodología estricta de sincronización de tiempos basada en el protocolo NTP.
- Herramientas forenses

Referentes nacionales e internacionales

Guías CIS: http://www.cisecurity.org/

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

NIST: National Institute of Standards and Technology, U.S. Department of Commerce
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER (CSRC): Publicaciones

INCIBE-CERT: Publicaciones

CMMC: Modelo CMMC — Office of the Under Secretary of Defense for Acquisition & Sustainment, Cybersecurity Maturity Model Certification

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

Veamos un ejemplo práctico de cómo deberían trabajar las tres áreas.

Fraude en transacciones a través de Servicios Digitales Financieros (DFS)

Presentación del tema

Nos encontramos ante un nuevo paradigma o nicho de mercado donde, los tradicionales servicios financieros, están migrando hacia servicios dependientes cien por ciento de las Telecomunicaciones.

Las autoridades y grandes holdings financieros están empujando fuertemente a la sociedad y empresas a hacer uso de ellos, pues les conviene en todo sentido.

El crecimiento de estos **Servicios Digitales Financieros** es vertiginoso, pero… El Usuario, la Banca y los Gobiernos necesitan y exigen **SEGURIDAD** y la masa de la responsabilidad sobre este tema la tienen las **"Telco"** y las **plataformas de pago**.

Fintech.

"Fintech" es un término amplio que define el uso de aplicaciones digitales, software, tecnología digital por parte de organizaciones financieras, bancos y startups. Pueden ir desde servicios de pagos, como ***Bizum*** o ***Twyp***, hasta sistemas de crédito al consumo como ***Movistar Money***.

¿Por qué nos interesa el tema?

Porque en un informe reciente de **ITU**, **ENISA** y todos los organismos financieros relevantes, donde se presenta el tema del Fraude en DFS es través de dos vías (ATTACK SURFACES) [1]:

- **SS7** (*principalmente por medio de:* ***SMS*** *y* ***USSD*** *– ambos son mensajes SS7*).

- **cellular air interface**

NOTA: Estas vías incluyen también la **SIM card**.

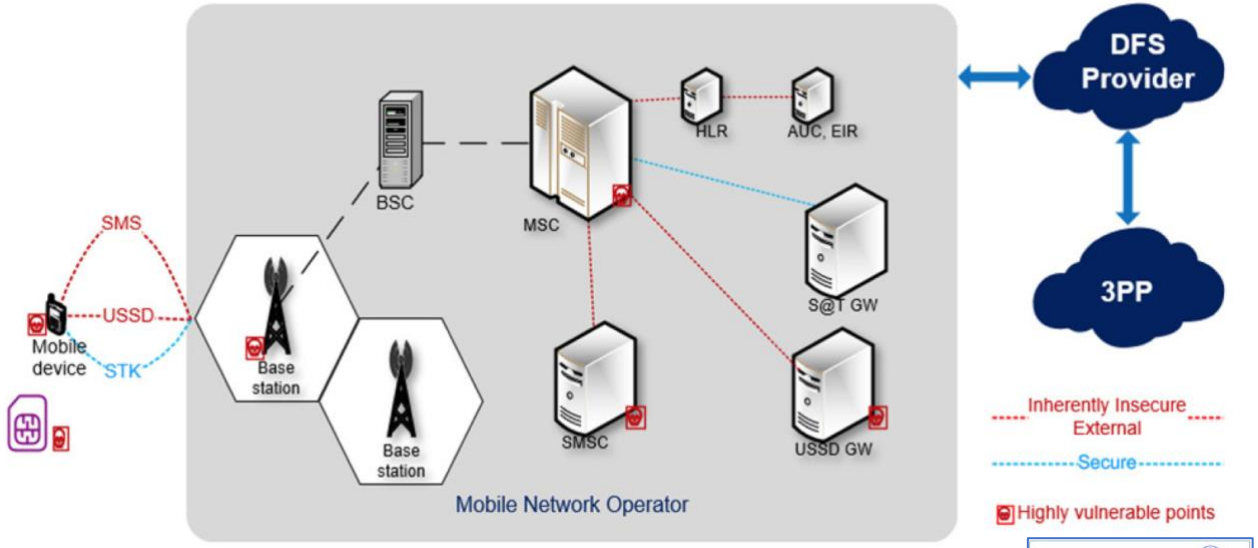


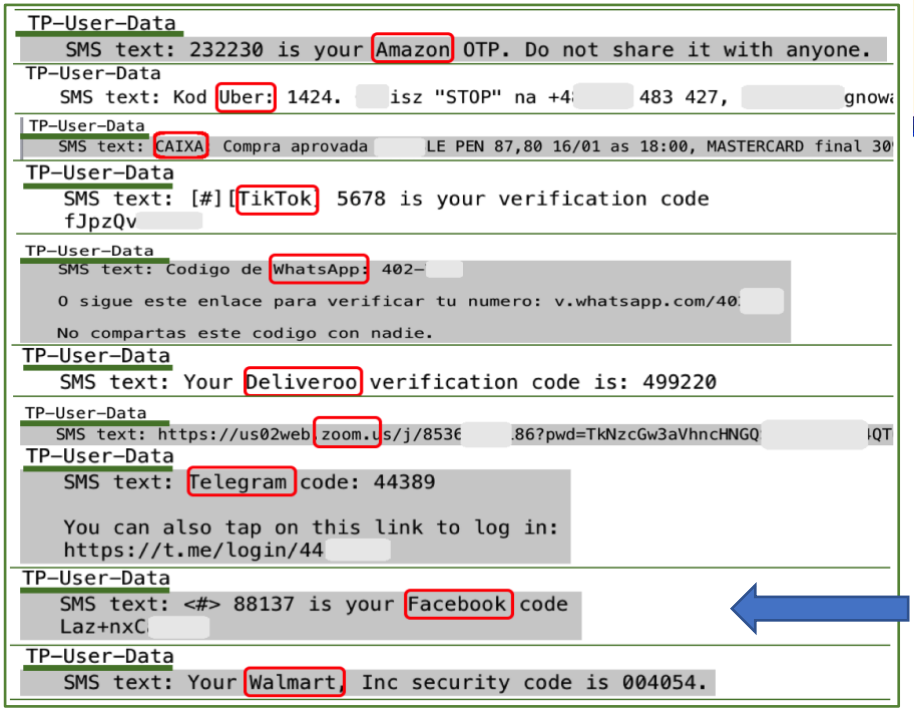
Imagen tomada del documento: 20-00383 Security testing for USSD and STK.pdf

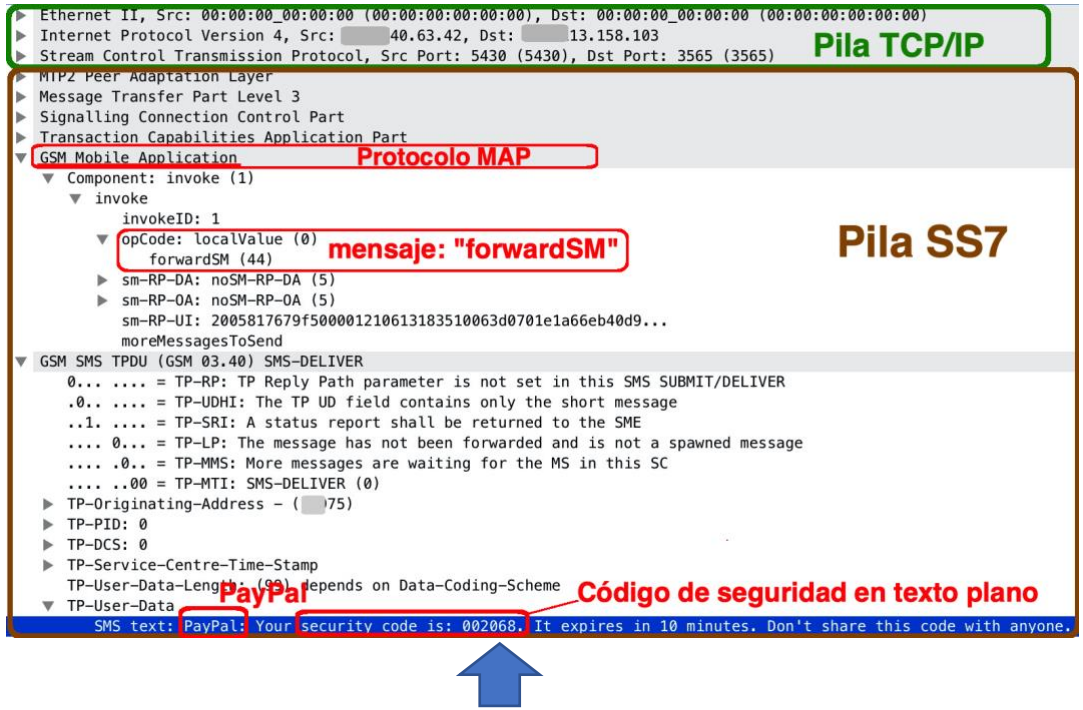
Ver detalle en libro "**Seguridad en Redes**"
www.darFe.es

[1] https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical-report-on-the-0SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f.pdf

Me encantaría dedicar más tiempo a esta idea pues sería importantísimo poder bajarla al terreno humanamente entendible, pero en estas líneas, no nos dará el tiempo, podéis buscar en Internet algunos artículos que he escrito sobre el tema.

Los problemas de estos servicios financieros, van relacionados con **mensajes SS7** de esta "red de voz", analicemos uno de ellos:





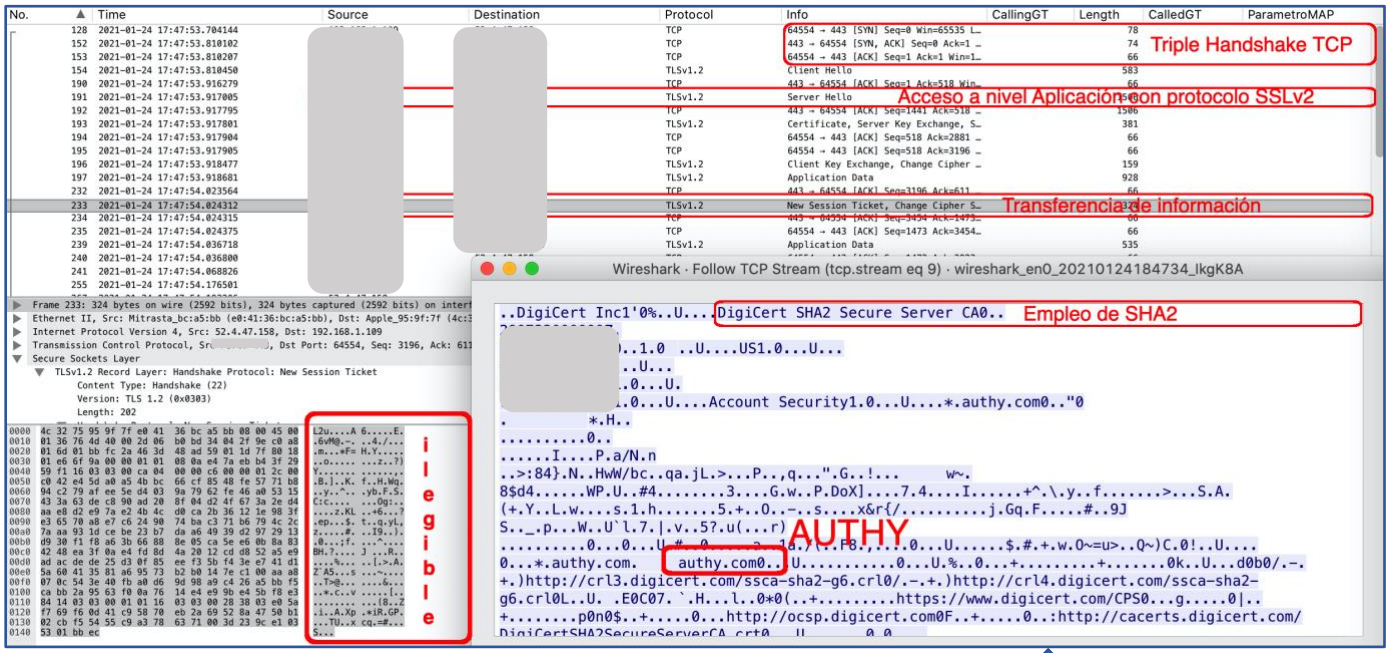
En la imagen superior, vemos la parte correspondiente a la pila **TCP/IP**, debajo de ella la parte de **SS7** y en este caso concreto, un mensaje SS7 cuyo "Operation Code" es: "**forwardSM**" y se corresponde con un factor de doble autenticación enviado por **PayPal**. El detalle que deseo que observéis (independientemente de las debilidades y ataques de la red SS7), es que estáis observando todo el contenido en **texto plano**.

Si analizamos únicamente el campo "**TP-User-Data**" en otras capturas de tráfico, vemos que estos mensajes SS7 en texto plano, son empleados por un sinnúmero de aplicaciones y empresas.

Comparemos un código enviado por **SS7** a través de un mensaje **SMS** contra un código generado por la red IP, a través de un **TOTP**, en este caso por medio de la aplicación "***Authy***".

En eta imagen podemos ver el triple handshake TCP, una vez finalizado ya pasa al nivel aplicación con el protocolo **SSLv2** empleando el algoritmo **SHA2**, en la ventana inferior de Wireshark, se ve perfectamente que el contenido es "**ilegible**".

En resumen, lo que se intenta presentar en los dos casos, es la gran diferencia entre continuar empleando la **red de voz** (con mensajes SS7) o ir migrando estos DFS hacia la **red de paquetes**, empleando todas las fortalezas que en la actualidad ofrece la pila **TCP/IP** (como en este caso por medio de SSL_v2).



Gobierno → Al ser informado, debe implementar medidas seguras.

Planificación → NO puede desconocer esta debilidad, debe mantenerse informado de estos temas y asesorar a:

Operación → Es el responsable de comprender estas capturas de tráfico y configurar adecuadamente las herramientas.

www.darFe.es

Muchas gracias

Alejandro Corletti Estrada