"Gobierno de la Ciberseguridad y estrategias resilientes"

México, agosto de 2021

Alejandro Corletti Estrada
(acorletti@DarFe.es - acorletti@hotmail.com)
www.darFe.es

TEMARIO DEL DÍA DE HOY:

1. Organización de la Ciberseguridad.
2. Lo crítico es la "Información"… no las Infraestructuras.
3. Concepto físico de Resiliencia.
4. Introducción a redes y sistemas Resilientes.
5. Análisis de Riesgo de Resiliencia.
6. Matriz de Resiliencia.
7. Procesos de ciberseguridad relacionados a Resiliencia.
8. Breves conceptos de Plan Director de Seguridad (*sobre la base de la resiliencia*).

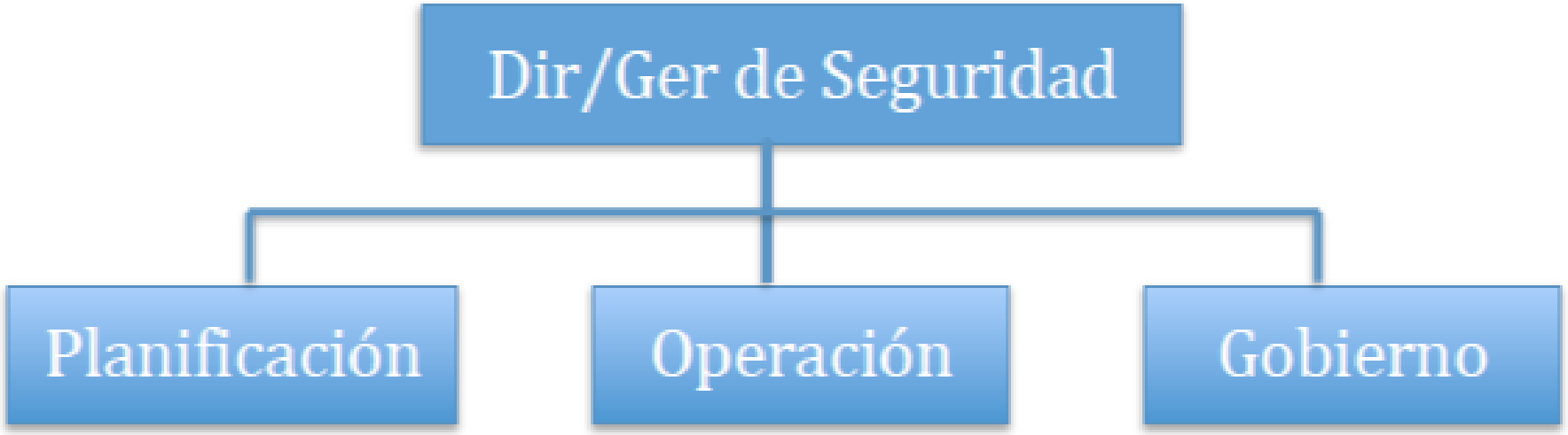
Bonus: Una visión de ciberseguridad a futuro y nuevos nichos de mercado (*Movilidad y Servicios Digitales Financieros {DFS}*)

1. Introducción

- 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:



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.

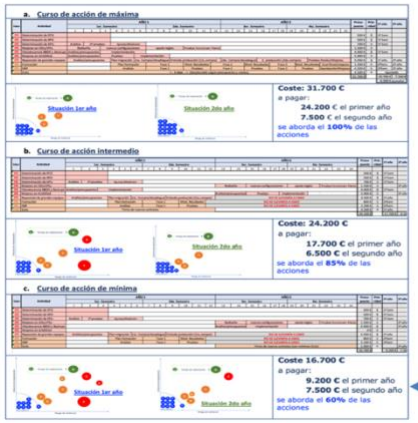
c. Controles.

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*



Cursos de acción

Según **INCIBE**:

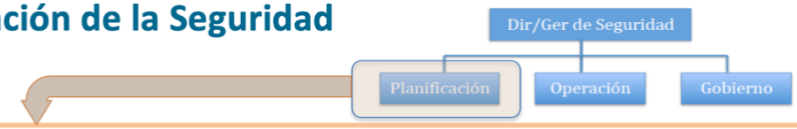
PLAN DIRECTOR DE SEGURIDAD

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?

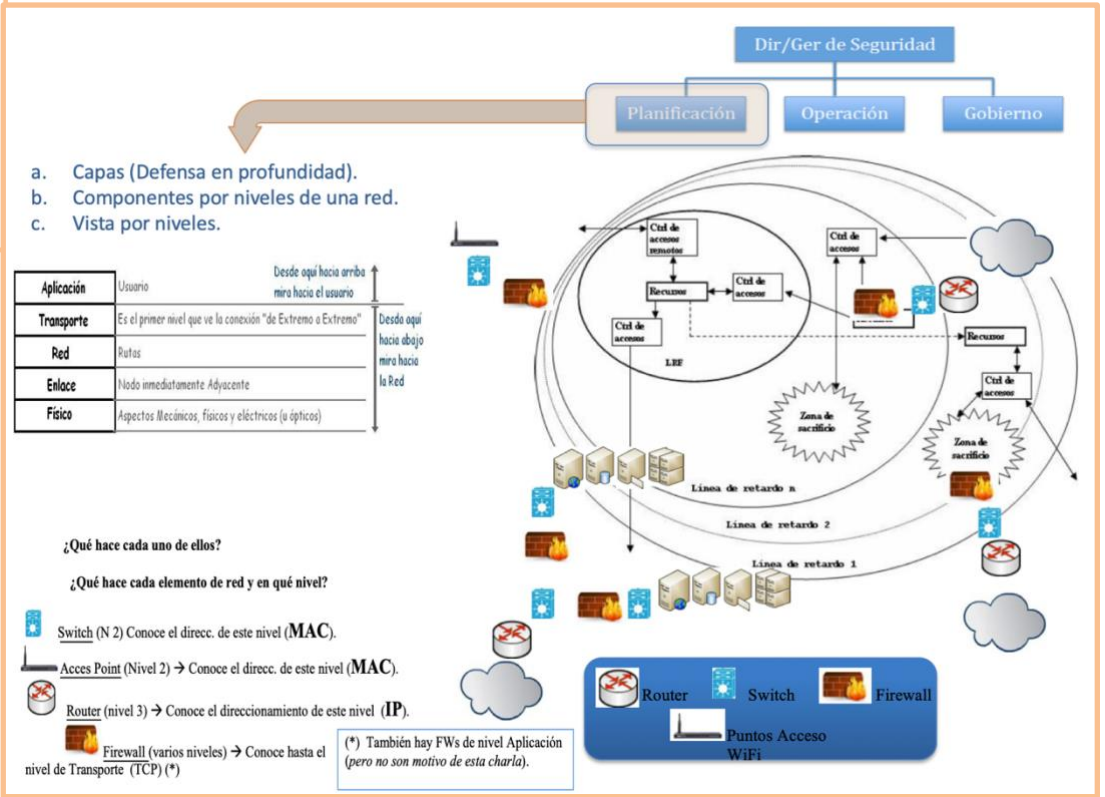
a. **Análisis técnico**. (Análisis de Viabilidad Técnica):
¿Qué subprocesos contempla?
a) Especificación Técnica de Requisitos funcionales, de Seguridad y de Gestionabilidad.
b) Informe de Análisis Técnico. (funcionalidad, escalabilidad, seguridad).
c) DTS (Definición Técnica de la Solución) Red Preliminar.

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	

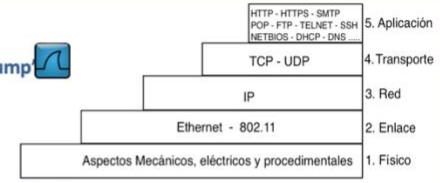
c. **Pruebas en Red** (Realización de las pruebas con tráfico real en primera instalación).
Si todo ha sido correcto los siguientes pasos serán:
a) Autorización de Introducción en planta para Despliegue.
b) Documentación de Despliegue.
c) Informe de Acreditación de Seguridad.
d) Informe de Pruebas FOA.



Operación de la Seguridad

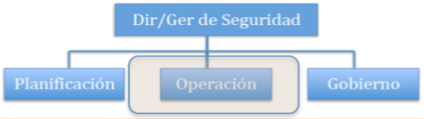
¿Qué debe hacer operación?

¿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

2. Lo crítico es la "Información"… no las Infraestructuras.

Estoy totalmente en desacuerdo con la postura que están tomando Instituciones y Estados al respecto, centrando la atención incorrectamente en la "materia" y no en lo "inmaterial".

Es momento que lo hagamos, debemos decir basta a lo físico y empezar a movernos en el mundo virtual, ese es el desafío principal para nuestras redes y sistemas de TI. Lo físico son las infraestructuras, lo virtual es la información, hoy debemos jugar nuestro combate.

2.1. Las regulaciones.

Reflexiones iniciales: El poder del siglo XXI se llama "**Información**".

El quinto escenario militar "Ciberespacio" tiene como límites la "**Información**"

El tesoro es la "**Información**", no la infraestructura que la sustenta.

(*No perdamos el norte sobre lo que hay que proteger*).

Detalle de la situación legal de la **UE** en libro: "**Manual de la Resiliencia**"

www.darFe.es

2.2. Lo crítico está en la Información.

Desde un punto de vista militar, a lo largo de la historia, se fueron definiendo escenarios o dominios militares, el primero fue "tierra", luego "agua", "aire", el siglo pasado se incorporó el "espacio", y este siglo el "**ciberespacio**" se estableció de común acuerdo mundial como el quinto escenario militar. Cabe mencionar que ya se está hablando de un sexto dominio que se trata del de "**opinión**" y es el tipo de guerra orientada a la opinión pública y cómo, de forma dirigida, se pueden generar tendencias y comportamientos. Este fenómeno se está tratando técnicamente desde hace años, se lo denomina "**CROWD**" (*multitudes*).

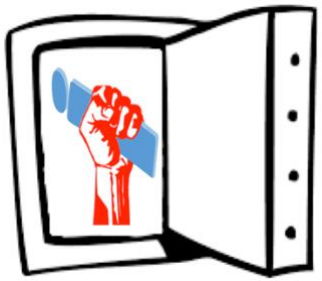
La definición de los cuatro primeros dominios trata de espacios físicos (tierra, mar, aire y el espacio), pero los dos que siguen son "no tangibles", más específicamente se los denomina "**escenarios virtuales**". No son reales, son intangibles. Concretamente lo que define al "**Ciberespacio**" es la Información (*nuevamente, no son las infraestructuras*), esta información debidamente dirigida a las "mentes" crea este sexto escenario de la "**opinión**".

Pero: **¿Qué es lo que se busca atacar?**

En TODO ataque lo que se está "**agregando** – **borrando** o **modificando**" es la "Información". La infraestructura de la organización o empresa será el efecto final.

*Las empresas líderes del mercado apuestan por el "poder de la Información". En estos momentos Google, Facebook, Whatsapp, apuestan por tener más y más "**Información**" que le permitan inferir o inducir tendencias (sexto escenario: "Opinión").*

2.3. La raíz del problema.



Cuando se unen:

- **el tiempo milenario**.

y

- **la experiencia muy afianzada**.

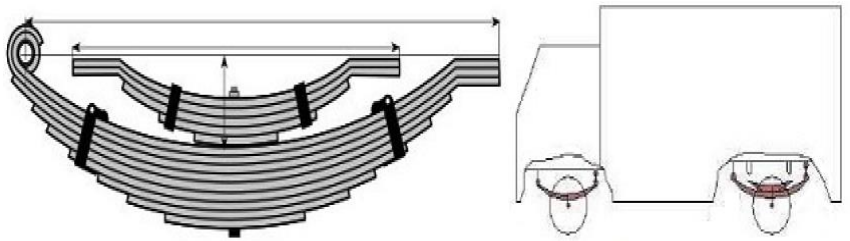
… A veces no es la mejor combinación, y arrastra una inercia difícil de revertir.

*Lo que vale es el **tesoro**… no la caja*

3. Concepto físico de Resiliencia.

Definición en ingeniería de resiliencia:

"La resiliencia es la propiedad que representa la capacidad de un material de recuperar su forma luego de sufrir una deformación".



Ballesta y Ballestín

Hace años se ha inventado el sistema de suspensión, por medio de elásticos, diseñados con flejes de acero en forma de arco, este tipo de sistemas se los suele llamar de "ballesta".

4. Introducción a redes y sistemas Resilientes.

Reflexionemos sobre algunos puntos de la resiliencia física:

- Reflexión 1: Límite (umbral) elástico, plástico o de rotura.
- Reflexión 2: Equilibrio entre rigidez y flexibilidad.
- Reflexión 3: Calidad del material (no necesariamente precio).
- Reflexión 4: Resiliente a qué.
- Reflexión 5: Amortiguación (rebote).
- Reflexión 6: Tiempo de respuesta óptimo.
- Reflexión 7: Esfuerzo de mantenimiento.
- Reflexión 8: Fisuras (o degradación).
- Reflexión 9: Grado de deformación.
- Reflexión 10: Presiones persistentes.

Ver detalle en libro:
"**Manual de la Resiliencia**"
www.darFe.es

Una infraestructura de redes y sistemas de TI no la podemos catalogar de resiliente o no resiliente. Me atrevería a afirmar que en ingeniería el término absoluto se acaba en los cálculos matemáticos y teorías, cuando llevamos el proyecto a la realidad, es preferible manejarse por valores de "tolerancia" o porcentajes de cumplimiento. Creo que lo más importante que he aprendido en mi formación de ingeniero es que: **Lo *perfecto* es enemigo de lo bueno**

Un ingeniero como mayor virtud debe tener la capacidad de encontrar los límites o umbrales. Cuánto más preciso sea en la definición de esos límites mayor será su capacidad ejecutiva

La clave es encontrar este compromiso que venimos planteando, para ello lo ideal es poder determinar cuál sería el "umbral de rotura" de nuestra infraestructura.

Por esta razón, es vital realizar el **análisis de riesgo** de forma metódica y sí, en particular, tomamos como referencia metodologías internacionalmente comprobadas, pues mejor que mejor.

> *"Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas"*
>
> **John Chambers** (ex *CEO de Cisco*).

5. Análisis de Riesgo de Resiliencia.

Si buscamos en Internet el significado, veremos que:

- riesgo: Contingencia o proximidad de un daño.
- arriesgar: Poner a riesgo.

  Exponer a una persona o cosa a un riesgo o ponerlos en peligro.

Secuencia natural de una Análisis de 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**

Ahora que hemos presentado los conceptos de análisis de riesgo, pongamos de manifiesto el título de:

*"**Análisis de Riesgo de Resiliencia**".*

6. Matriz de Resiliencia.

Iniciaremos este capítulo, agrupando nuestras diez reflexiones en tres grupos.

- Objetivos y gestión
- Ciclo de vida
- Arquitectura de ciberdefensa

Asignaremos en los mismos las reflexiones de acuerdo al siguiente criterio.

Objetivos y gestión:

Reflexión 4: Resiliente a qué.
Reflexión 5: Amortiguación (rebote).
Reflexión 7: Esfuerzo de mantenimiento.

Ciclo de vida:

Reflexión 1: Límite (umbral) elástico, plástico o de rotura.
Reflexión 6: Tiempo de respuesta óptimo.
Reflexión 8: Fisuras (o degradación).
Reflexión 9: Grado de deformación.

Arquitectura de ciberdefensa:

Reflexión 2: Equilibrio entre rigidez y flexibilidad.
Reflexión 3: Calidad del material.
Reflexión 10: Presiones persistentes.

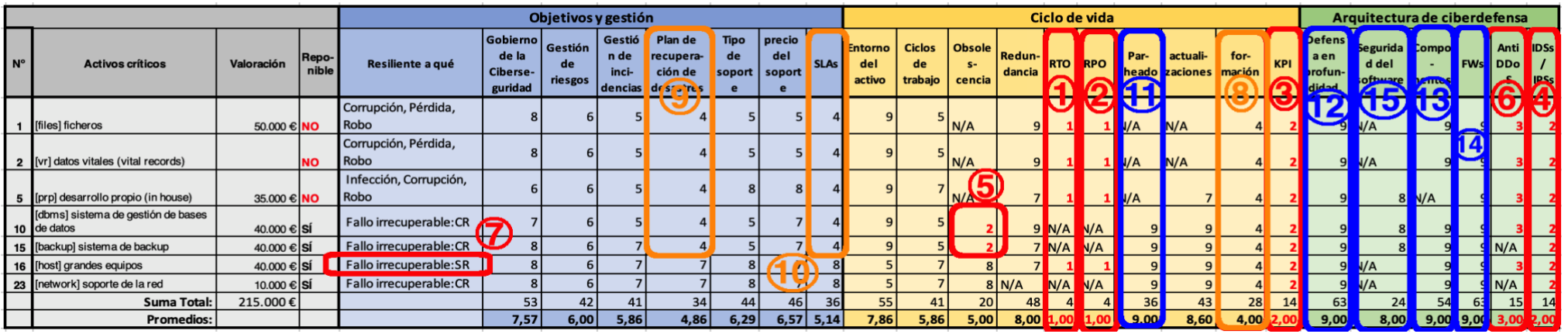
Para poder ir determinando la resiliencia, proponemos incorporar a cada uno de nuestros tres grupos las siguientes ideas:

Objetivos y gestión	**Ciclo de vida**	**Arquitectura de ciberdefensa**
Reflexión 4: Resiliente a qué. Reflexión 5: Amortiguación (rebote). • Gobierno de la Ciberseguridad. • Gestión de riesgos. • Gestión de incidencias. • Plan de recuperación de desastres Reflexión 7: Esfuerzo de mantenimiento. • Tipo de soporte. • precio del soporte. • SLAs	Reflexión 1: Límite (umbral) elástico, plástico o de rotura. • Entorno del activo. • Ciclos de trabajo. • Obsolescencia. • Redundancia. Reflexión 6: Tiempo de respuesta óptimo. • Gestión de copias de respaldo y recuperación. • RTO (Restauration Time Objetive). • RPO (Restauration Point Objetive). Reflexión 8: Fisuras (o degradación). • Parcheado. • Actualizaciones. • Formación Reflexión 9: Grado de deformación. • KPI - Indicadores Clave de Desempeño	Reflexión 2: Equilibrio entre rigidez y flexibilidad. • Defensa en profundidad. Reflexión 3: Calidad del material (no necesariamente precio). • Diseño. • Seguridad del software. • Componentes. Reflexión 10: Presiones persistentes. • Firewalls. • AntiDDoS. • IDSs/IPSs.

Podemos desarrollar una sencilla plantilla de cálculo que nos permita tener una foto inicial de cómo veo reflejado el conjunto. Para seguir profundizando en el tema, pongamos un ejemplo de ello.

				Objetivos y gestión								Ciclo de vida									Arquitectura de ciberdefensa					
Nº	Activos críticos	Valoración	Repo-nible	Resiliente a qué	Gobierno de la Ciberse-guridad	Gestión de riesgos	Gestión de inci-dencias	Plan de recupera-ción de desastres	Tipo de soport e	precio del soport e	SLAs	Entorno del activo	Ciclos de trabajo	Obsole s-cencia	Redun-dancia	RTO	RPO	Par-cheado	actuali-zaciones	for-mación	KPI	Defens a en profun-didad.	Segurida d del software	Compo - nentes	FWs	Anti DDo S	IDSs / IPSs
1	[files] ficheros	50.000 €	NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
2	[vr] datos vitales (vital records)		NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
5	[prp] desarrollo propio (in house)	35.000 €	NO	Infección, Corrupción, Robo	6	6	5	4	8	8	4	9	7	N/A	7	1	1	N/A	7	4	2	9	8	N/A	9	3	2
10	[dbms] sistema de gestión de bases de datos	40.000 €	SÍ	Fallo irrecuperable:CR	7	6	5	4	5	7	4	9	5	2	9	N/A	N/A	9	9	4	2	9	8	9	9	3	2
15	[backup] sistema de backup	40.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	4	5	7	4	9	5	2	7	N/A	N/A	9	9	4	2	9	8	9	9	N/A	2
16	[host] grandes equipos	40.000 €	SÍ	Fallo irrecuperable:SR	8	6	7	7	8	7	8	5	7	8	7	1	1	9	9	4	2	9	N/A	9	9	3	2
23	[network] soporte de la red	10.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	7	8	7	8	5	7	8	N/A	N/A	N/A	9	9	4	2	9	N/A	9	9	N/A	2
	Suma Total:	215.000 €			53	42	41	34	44	46	36	55	41	20	48	4	4	36	43	28	14	63	24	54	63	15	14
	Promedios:				7,57	6,00	5,86	4,86	6,29	6,57	5,14	7,86	5,86	5,00	8,00	1,00	1,00	9,00	8,60	4,00	2,00	9,00	8,00	9,00	9,00	3,00	2,00

El objetivo fundamental de esta propuesta es avanzar en nuestra "**Matriz de Resiliencia**" tal cual lo propone la familia ISO/UNE 27000, paso a paso generemos un ciclo de mejora continua de la seguridad.



Hagamos un análisis más de la plantilla recientemente presentada.

a. Curso de acción de máxima

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas			Ajustes/Medición																			700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs			Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta													1.500 €	3		
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS	Análisis/presupuestos			Pruebas			Implementación																		5.000 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración	1ra. Compra/despliegue			Entrada producción (1ra.compra)					2da. Compra/despliegue			E. producción (2da.compra)				Pruebas finales/Mejoras					9.000 €	1	1º año	2º año
(8)	Formación				Plan formación			Fase 1			Med. Resultados			Fase 2			Med. Resultados			Fase 3		Med. Resultados		Eval fimal/mejoras		1.500 €	5	2ºSem	2º año
(9)	DRP				Análisis			Fase 1			Pruebas			Fase 2			Pruebas			Fase 3		Pruebas		Aprobación/Mejoras		4.500 €	5	2ºSem	2º año
(10)	SLAs	<-- 1 mes --> (desplazable según presupuesto y costes)																								4.500 €	4	Ajustable	
																										31.700 €		19.700 €	7.500 €
																												4.500 € (ajustable)	

Coste: 31.700 €
a pagar:
24.200 € el primer año
7.500 € el segundo año
se aborda el **100%** de las acciones

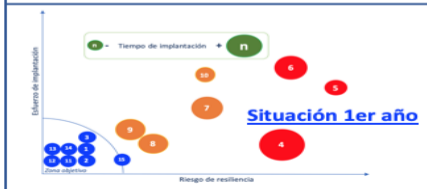
b. Curso de acción intermedio

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas			Ajustes/Medición																			700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta		1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS													Análisis/presupuestos			Pruebas			Implementación						5.000 €	3		2º año
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración	1ra. Compra/despliegue		Entrada producción (1ra.compra)			NO SE LLEVARÍA A CABO															4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1		Med. Resultados	NO SE LLEVARÍA A CABO															800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1		Pruebas	NO SE LLEVARÍA A CABO															2.200 €	5	2ºSem	
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año	
																										24.200 €		17.700 €	6.50

Coste: 24.200 €
a pagar:
17.700 € el primer año
6.500 € el segundo año
se aborda el **85%** de las acciones

c. Curso de acción de mínima

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas			Ajustes/Medición																			700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta		1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups													Análisis/presupuestos			Implementación									4.000 €	2		2º año
(6)	Mejoras en AntiDDoS																									0 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración	1ra. Compra/despliegue		Entrada producción (1ra.compra)			NO SE LLEVARÍA A CABO															4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1		Med. Resultados	NO SE LLEVARÍA A CABO															800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1		Pruebas	NO SE LLEVARÍA A CABO															2.200 €	5	2ºSem	
(10)	SLAs													Firma de nuevos contratos (con mínimos SLAs)												2.000 €	4		2º año
																										16.700 €		9.200 €	7.50



Coste 16.700 €
a pagar:
9.200 € el primer año
7.500 € el segundo año
se aborda el **60%** de las acciones

La decisión que adopte la dirección de mi empresa, será la:

"**Estrategia de Resiliencia**" que adoptaremos para los próximos dos años.

Nuevamente ver detalle en libro:
"**Manual de la Resiliencia**"
www.darFe.es

7. Procesos de ciberseguridad relacionados a Resiliencia.

El **Centro Cripotológico Nacional** de España (**CCN**), que es un organismo de reconocido prestigio nacional e internacional dependiente del Centro Nacional de Inteligencia (**CNI**).

Dentro de la página Web del CCN podéis encontrar información de muy buena calidad: https://www.ccn.cni.es/index.php/es/

A su vez, una de las responsabilidades del CCN es el **CERT** (Computer Emergency Response Team), que en España, se lo conoce como "CCN-CERT": https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es.

En la misma figuran todas las guías de seguridad del ENS (Esquema Nacional de Seguridad), las cuáles son de gratuita descarga y no me canso de recomendar por su nivel de excelencia. Se las reconoce como la "**familia 800**", podéis descargarlas en:

Existen al menos los siguientes procedimientos que NO pueden faltar en una arquitectura Ciberresiliente:

1	Gobierno de la Ciberseguridad	9	Control de accesos
2	Plan de recuperación de desastres (DRP: Disaster Recovery Plan)	10	Entrada en Producción
3	Plan de Continuidad de Negocio	11	Seguridad en la comunicaciones
4	Gestión de la información (Clasificación y tratamiento)	12	Responsabilidades, obligaciones y funciones del personal
5	Gestión de copias de respaldo y recuperación	13	Gestión de terceros (proveedores, partners y clientes)
6	Gestión de riesgos	14	Cumplimiento legal
7	Gestión de incidentes	15	Gestión del ciclo de vida
8	Gestión de cambios y actualizaciones	16	Análisis forense

8. Breves conceptos de Plan Director de Seguridad *(sobre la base de la resiliencia)*.

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

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. incibe

- Tres referencias importantes (**CMMC-ISO27002-ENS**)
- Identificamos una situación inicial, con su riesgo e impacto (*Fase 1 flujo **INCIBE***)
- Calculamos el riesgo e impacto de la "información crítica" (*libro "**Manual de la Resiliencia**"*)
- Generamos cursos de acción (al menos bianuales) para que la Dirección decida (*ver Cap 8. Matriz de Resiliencia del libro mencionado*).
- Evaluamos y obtuvimos la foto inicial sobre la base de los niveles de madurez de **CMMC**.
- Definimos las métricas adecuadas sobre la base de **ISO-27004** (*ver Cap. 10. Ciclo de Vida del libro mencionado*).
- Planificamos y agendamos "hitos de control" y supervisión, sobre los objetivos de madurez de CMMC.
- Aprobación y firma el PDS.
- Vamos adoptando las acciones de mejora y solucionando los desvíos en cada ciclo de vida.

En el artículo "Plan Director de Seguridad (una visión: práctica, eficiente y estándar)" se presenta una comparativa de:

- Dominios **CMMC** *(Cybersecurity Maturity Model Certification)*
- Grupos de control de **ISO 27002**
- Dimensiones del **ENS** *(Esquema Nacional de Seguridad)*

La idea es evaluar diferencias y modelar un plan sin dejar de lado ningún aspecto de estas referencias internaciones.

En el año 2018, publiqué un artículo llamado:

Esquema Nacional de Seguridad e ISO 27001
¿Cómo implantar ambos en mi empresa? (podéis descargarlo AQUí)

Relacionaba los pasos a seguir sobre una publicación de **INCIBE**.

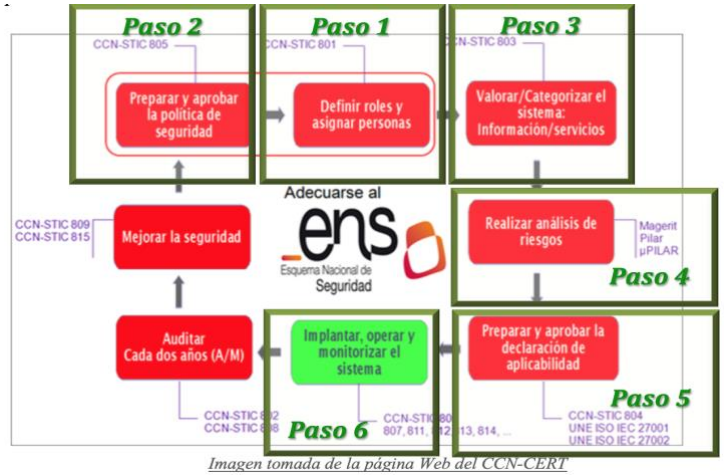
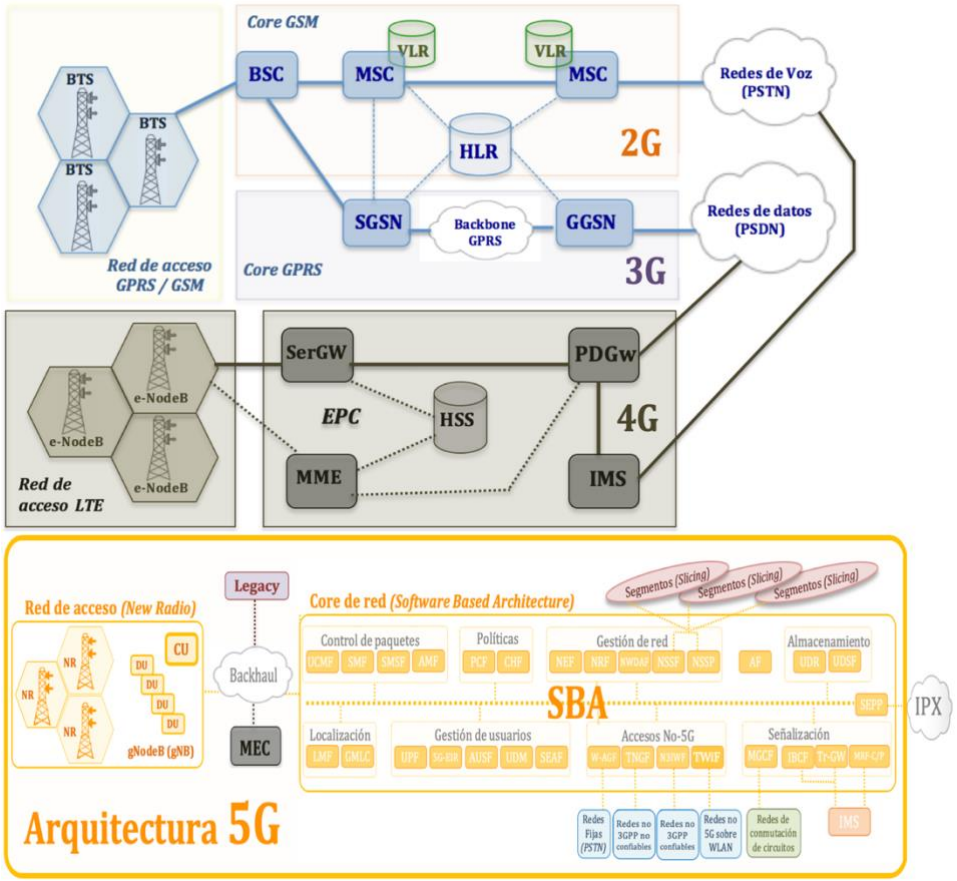


Imagen tomada de la página Web del CCN-CERT

***Bonus*: Una visión de ciberseguridad a futuro y nuevos nichos de mercado**

a. Movilidad

- Las **redes móviles** fueron evolucionando de forma acelerada, mejorando sus prestaciones año a año.
- Ya conocemos **4G** como una tecnología que nos ha abierto el mercado de la "**Movilidad**".
- En virtud de la pandemia todos hemos visto que el teletrabajo ha llegado para quedarse y este fenómeno es irreversible.
- El despliegue e implantación de **5G** es una realidad que en Europa y EEUU ya se comercializa y se está empleando.



- **5G** por primera vez iguala el ancho de banda, la latencia y la confiabilidad respecto a la "red fija".
- **5G** tiene muchas nuevas funcionalidades que nos abren nichos de mercado a las empresas relacionadas a Telco:

  Segmentos (Slicing):

  - mMTC: massive Machine Type Communication → IoT
  - eMBB: enhanced Mobile Broadband (eMBB) → Eventos
  - URLLC: Ultra-Reliable Low Latency Communications → Salud
  - Vehículo a X (V2X: Vehicle to X → Vehículos autónomos.

  MEC (Multi-access Edge Computing)

  Virtualización:

  - NFV (Network Function Virtualization)

- SDN (Software Defined Networks)
- SDO (Software Defined Operations)
- SDR (Software Defined Radios)
- OpenRAN
- Cloud

FWA (Fixed Wireless Access)

- 5G FWA debe verse como una oportunidad que depende en gran medida de las realidades locales.
  1) Equipos fijos o semi fijos en locales residenciales
  2) Equipos fijos o semi fijos en locales comerciales
  3) Unidades FWA como conectividad de respaldo para empresas
  4) Soluciones FWA como backhaul para Small Cells

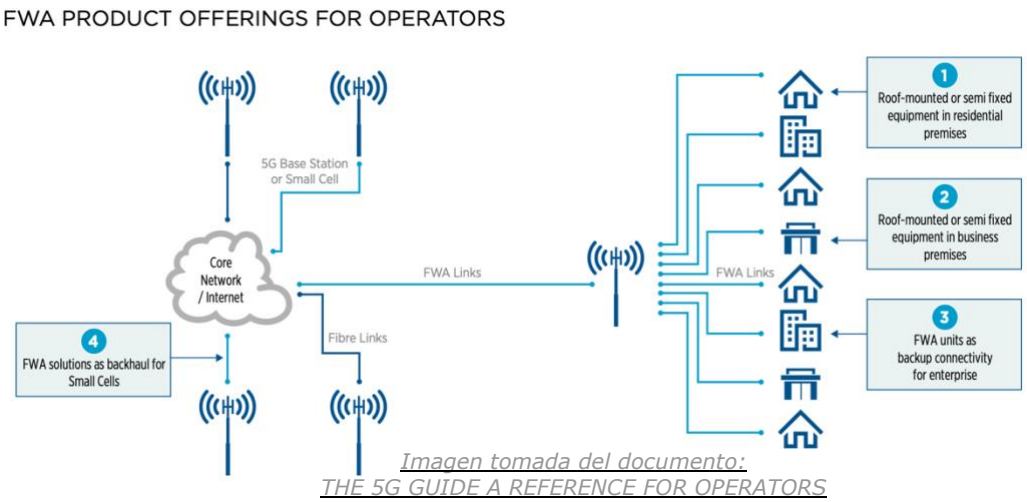


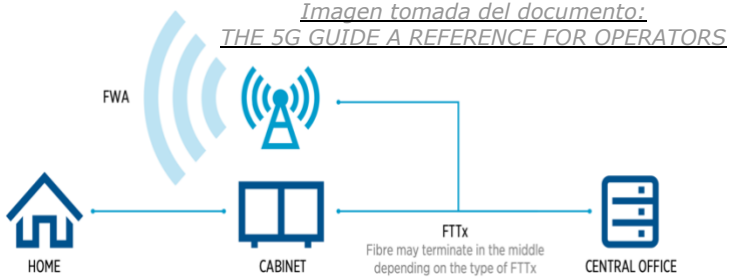
Imagen tomada del documento:
THE 5G GUIDE A REFERENCE FOR OPERATORS

Dos conceptos nuevos que se comenzaron a emplear sobre los tendidos de telecomunicaciones son:

- **Brownfield**: Zonas donde ya hay instalaciones de voz y/o datos sobre cables de cobre.
- **Greenfield**: Zonas de nueva o reciente construcción, donde aún no existe cobre.

FWA es una alternativa de menor costo que Greenfield FTTx

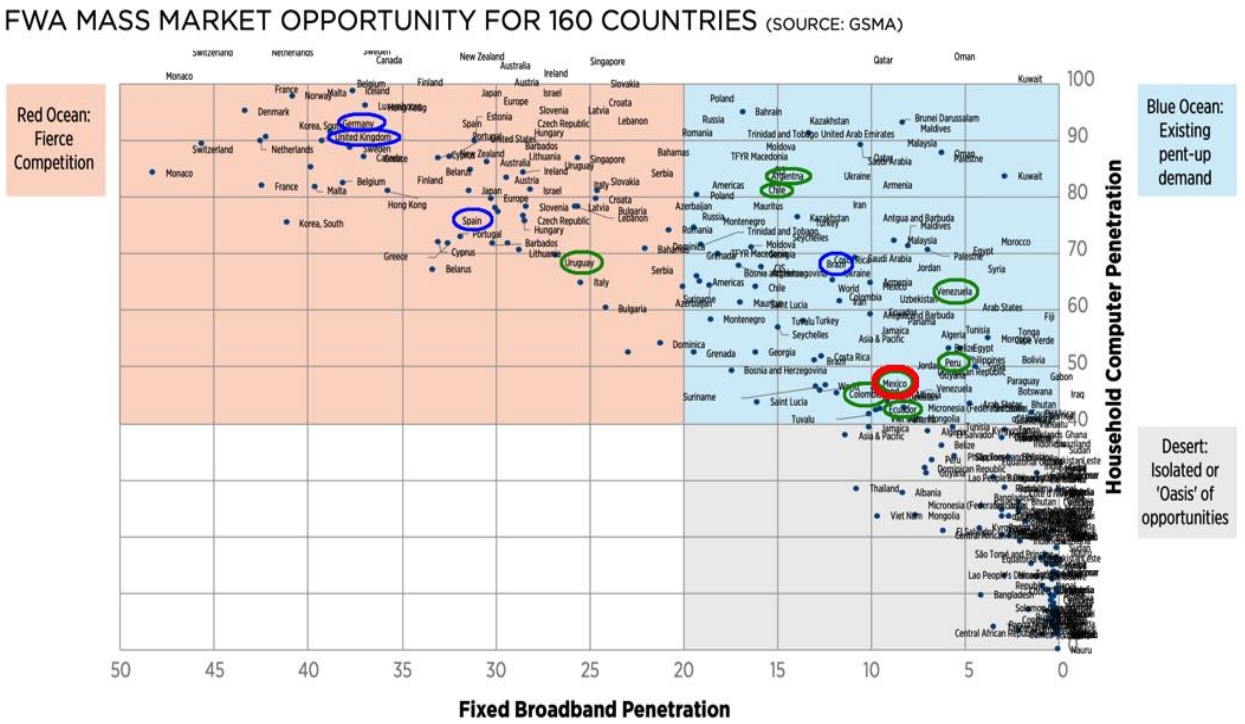
Imagen tomada del documento:
THE 5G GUIDE A REFERENCE FOR OPERATORS



"Competencia estratégica" con banda ancha fija.

Existe un debate en la industria en curso sobre las ventajas de utilizar FWA para competir con las propuestas existentes de banda ancha fija.

La figura que sigue muestra un gráfico de **160 países** sobre la penetración de ordenadores en los hogares y la penetración de banda ancha fija, y muestra que para FWA, la mayoría de los mercados se pueden clasificar como Red Ocean, **Blue Ocean** o Desert.



b. Servicios Digitales Financieros (DFS)

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**".

"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***.

Tendencias de Servicios Financieros.

La industria de servicios financieros, especialmente la industria bancaria, se está convirtiendo cada vez más en un negocio de tecnología. Más que nunca, la competitividad de varios productos centrados en las finanzas se diferencia por las soluciones tecnológicas que los habilitan

1. ¿Qué son los Servicios Financieros Digitales? (**DFS**: Digital Financial Services).

Los servicios financieros digitales (**DFS**) incluyen una amplia gama de servicios a los que se accede y se prestan a través de canales digitales, incluidos pagos, crédito, ahorros, remesas y seguros. El concepto DFS incluye servicios financieros móviles (**MFS**).

MFS es el uso de un teléfono móvil para acceder a servicios financieros y ejecutar transacciones. MFS incluye: M-Banking, M-payments, M-money.

- **M-Money** es un servicio móvil que facilita las transferencias electrónicas y otros servicios que utilizan redes móviles.
- **M-payments** es el servicio concreto de pagos por móvil (ejemplo: Mobile Pay).
- **M-Banking** es el uso de un teléfono móvil para acceder a servicios bancarios y ejecutar transacciones financieras. - A menudo se utiliza para referirse solo a clientes con cuentas bancarias.

Tres modelos de negocio:

- **Modelo dirigido por el banco** (generalmente: Mobile Virtual Network Operator: **MVNO**)
- **Modelo liderado por MNO** (Mobile Network Operator) (por ejemplo, Airtel Money, MPESA)
- **Modelo independiente** (por ejemplo, bKash) no son bancos, ni MNO.

Este modelo de negocio, presenta situaciones "mix" pues hay bancos que ya son **MVNO**, como es el caso de **SberBank,** (Rusia) y hay **MNO** que buscan nichos de mercado financieros, como es el caso de **Movistar Money** (España) que ofrece financiamiento a sus subscriptores a través de "Telefónica Consumer Finance" (*Entidad financiera constituida "a pachas" entre **Telefónica** y **CaixaBank***).

Existen también importantes alianzas como es el caso de **Bizum**, conformada por la unión de 27 bancos Españoles.

Lo que se destaca en todos estos casos es el **doble factor de autenticación** que emplean casi todos ellos, y es el tema central.

2. ¿Por qué nos interesa todo lo desarrollado anteriormente?

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**

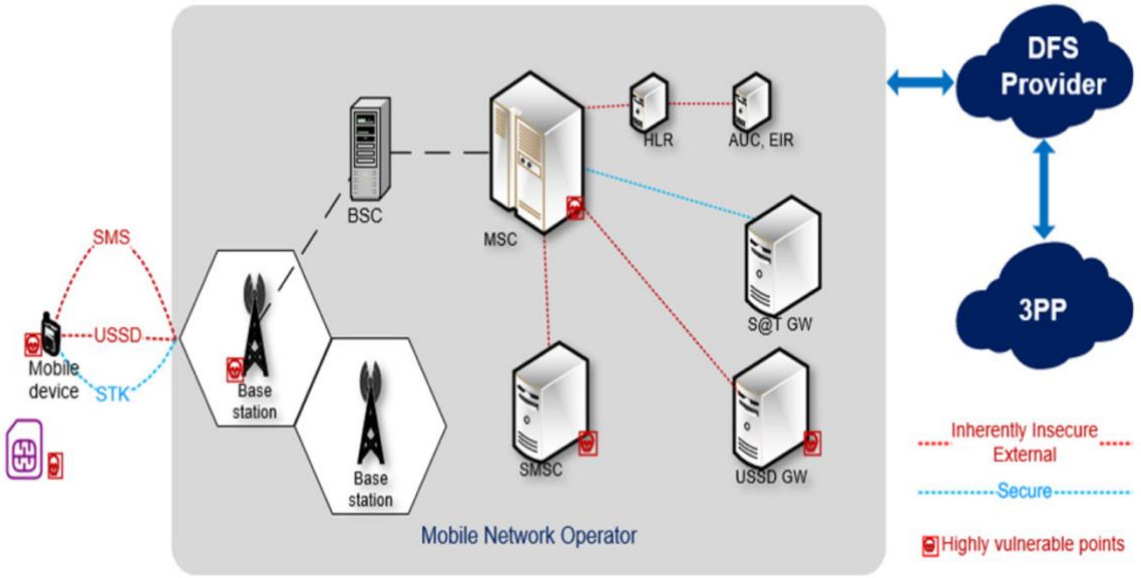


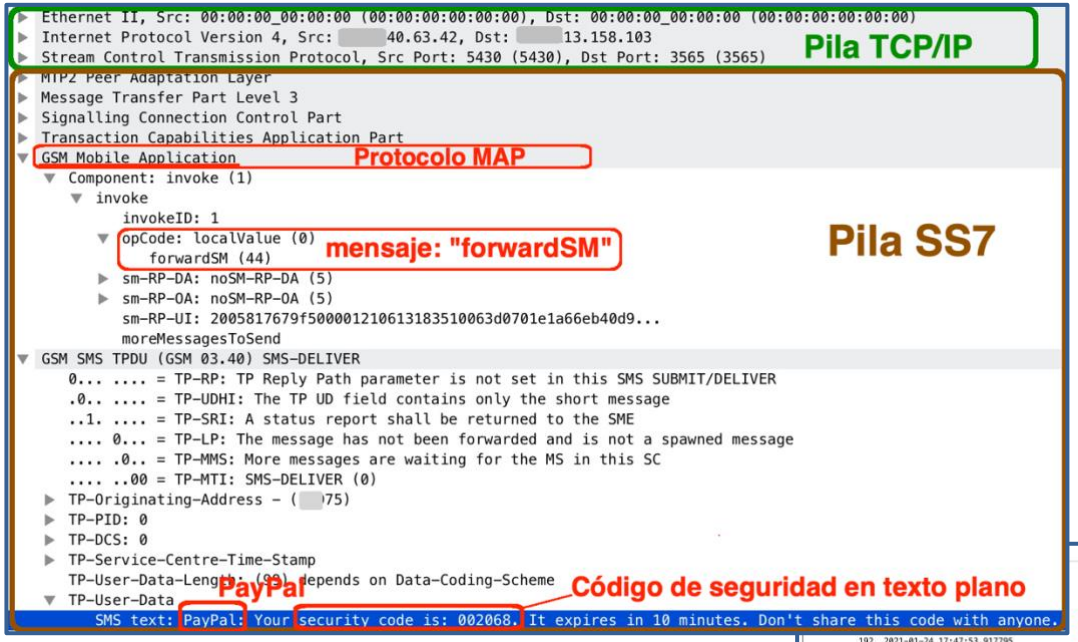
Imagen tomada del documento: 20-00383 Security testing for USSD and STK.pdf

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

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

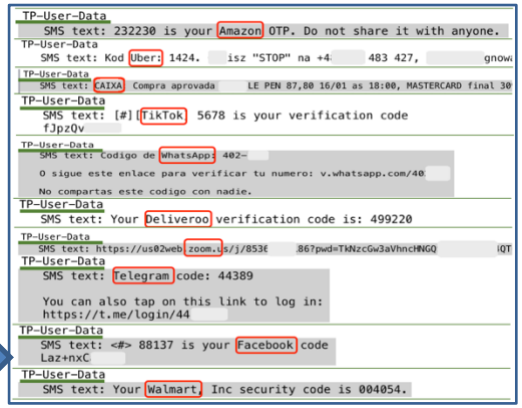
Doble factor de autenticación.



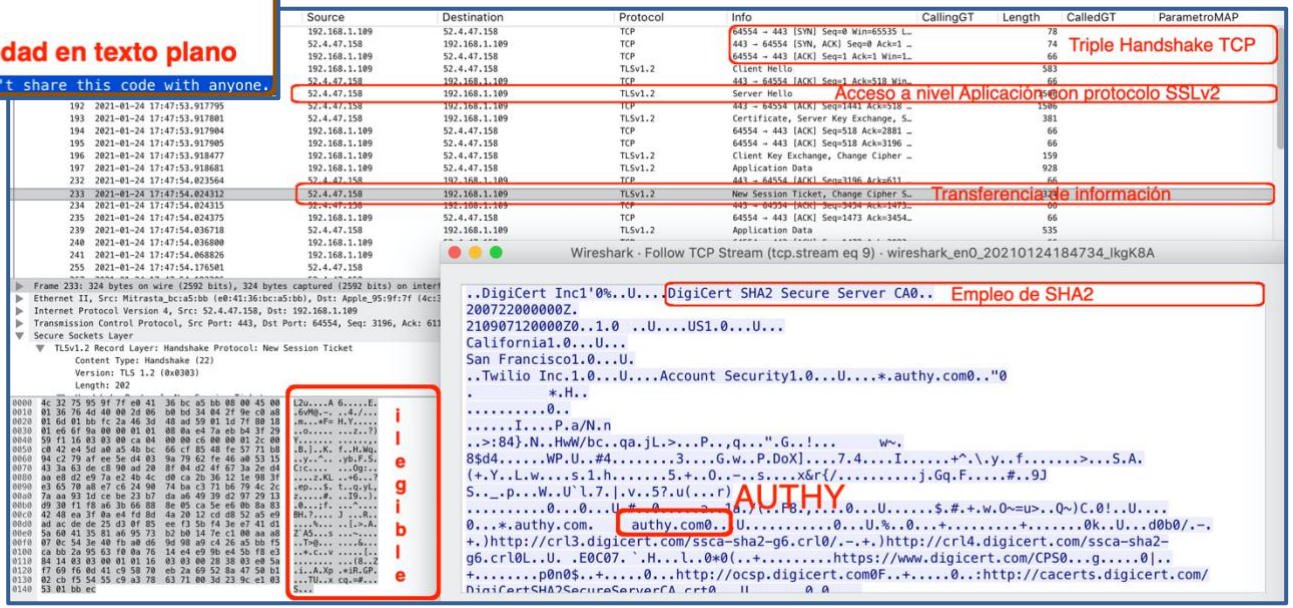
En la imagen de nuestra izquierda, estamos viendo la captura de tráfico de un mensaje de doble factor de autenticación enviado, en este caso por "**Paypal**".

Como puede apreciarse en la última línea todo el mensaje viaja en "texto plano", código de seguridad incluido.

Mismo caso con ***Uber, Caixa, TikTok, Whathsapp, Deliveroo, Zoom, Telegram, Facebook, Wallmart…***



Comparemos en la imagen de la derecha, 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***".



Muchas gracias

agosto de 2021

Alejandro Corletti Estrada
(acorletti@DarFe.es - acorletti@hotmail.com)
www.darFe.es