Charla Diplomatura Universitaria en gestión de la Ciberdefensa.

Argentina 22 de noviembre de 2022

Recursos gratuitos:

- **Curso Gratuito de** "Técnico en Ciberseguridad"
- **Ciclo** "Aprendiendo Ciberseguridad paso a paso"
- Cuatro libros de gratuita descarga en formato electrónico.
- Cientos de artículos, videos y capturas de tráfico
- Canal Youtube.

Curso Gratuito de:

"Técnico en Ciberseguridad"

Ciclo "Aprendiendo Ciberseguridad paso a paso"

Cientos de artículos, videos y capturas de tráfico

Canal Youtube:

DarFe Learning Consulting Canal Youtube

Cuatro libros de gratuita descarga en formato electrónico:

- Seguridad por Niveles
- Seguridad en Redes
- Ciberseguridad, una estrategia Informático/Militar
- Manual de la Resiliencia

Las Redes de Telecomunicaciones

La comunicación a distancia ha vivido una importante transformación desde el siglo XIX. Telégrafos, centralitas manuales, líneas de ocho kilómetros y teléfonos fijos han evolucionado hasta transformarse en la comunicación instantánea, permanente y global que conocemos en la actualidad.

Joseph Henry

Telégrafo 1831

Hermanos Lumière

Cinematógrafo 1895

TV 1923

Computador 1946

Narinder Singh Kapany, John Tyndall

Fibra Óptica 1952

Arpanet 1969

xDSL 1997

3G

Wi Fi 2000

Smartphones 2007

5G 2020

1857 Teléfono

Antonio Meucci

1897 Radio

Nikola Tesla
Julio Cervera

1937 Radio-telescopio

Grote Reber

1946 Móvil

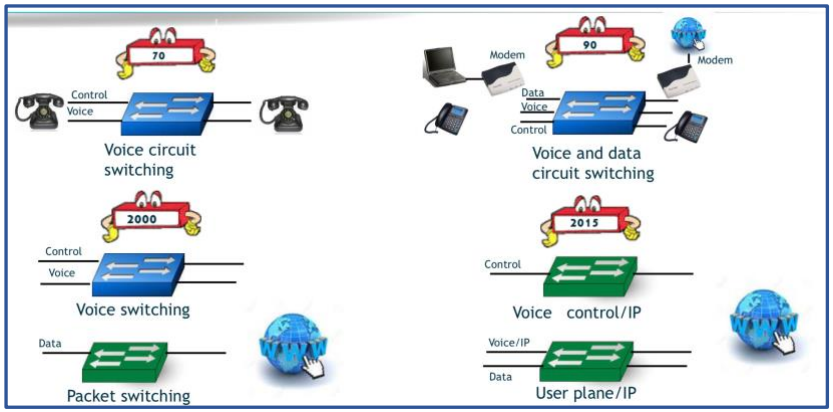
1957 Satélite

1981 PC

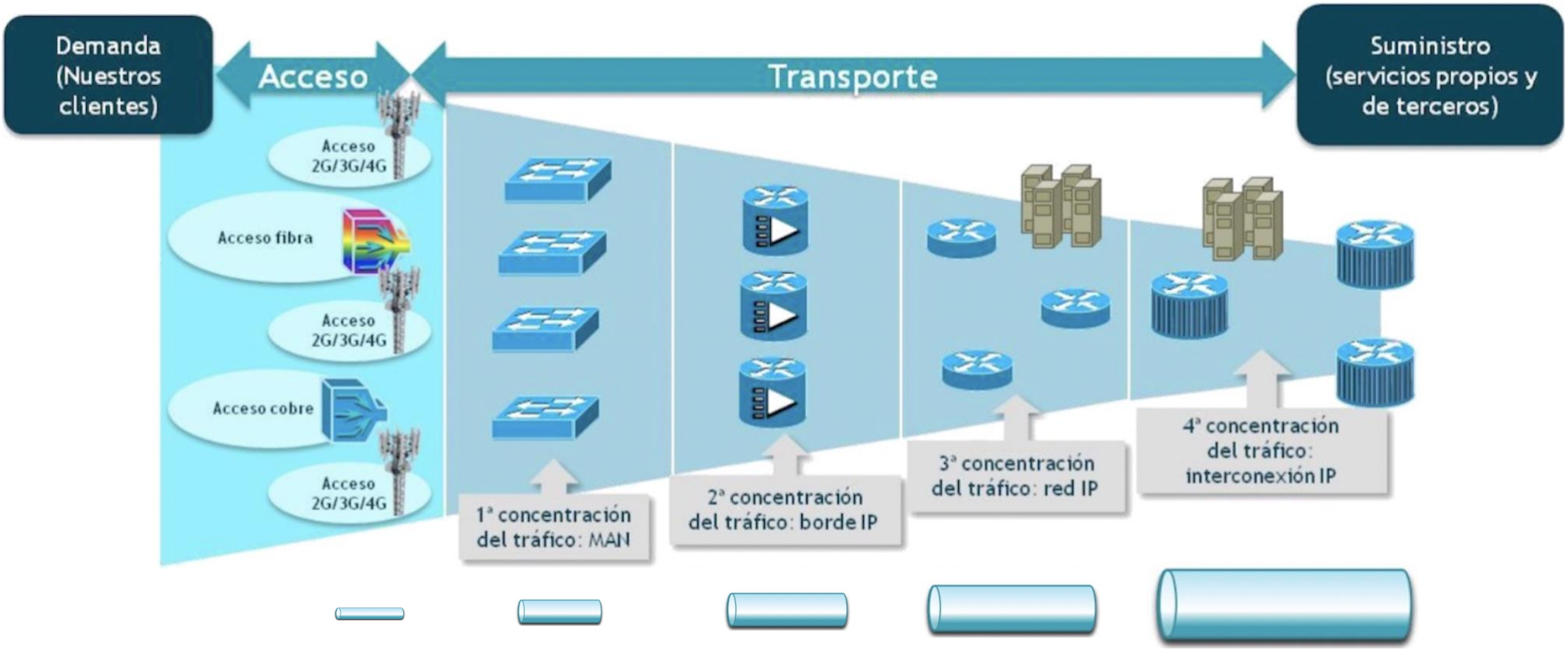
1998 Google

2004

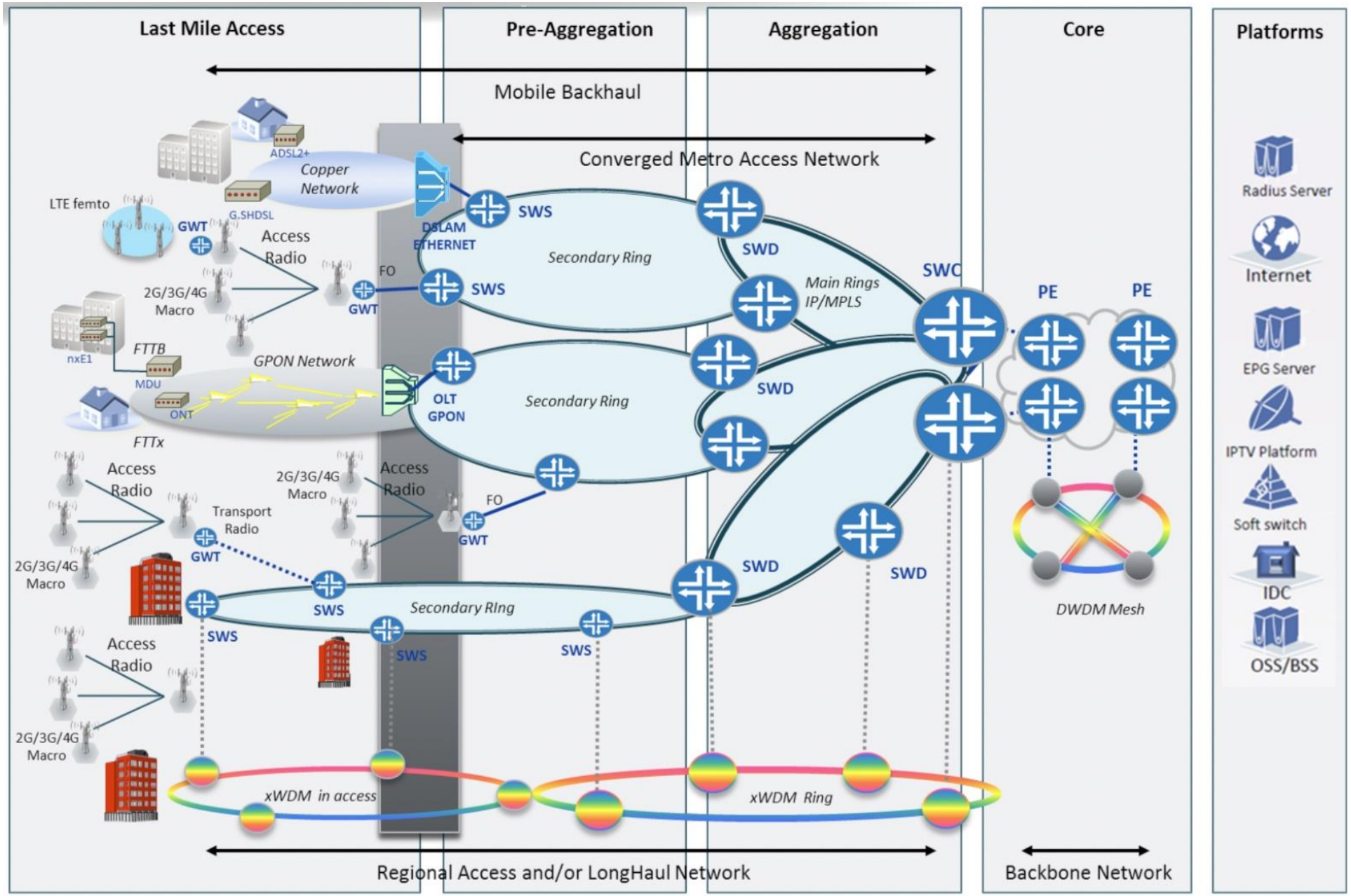
2009 4G



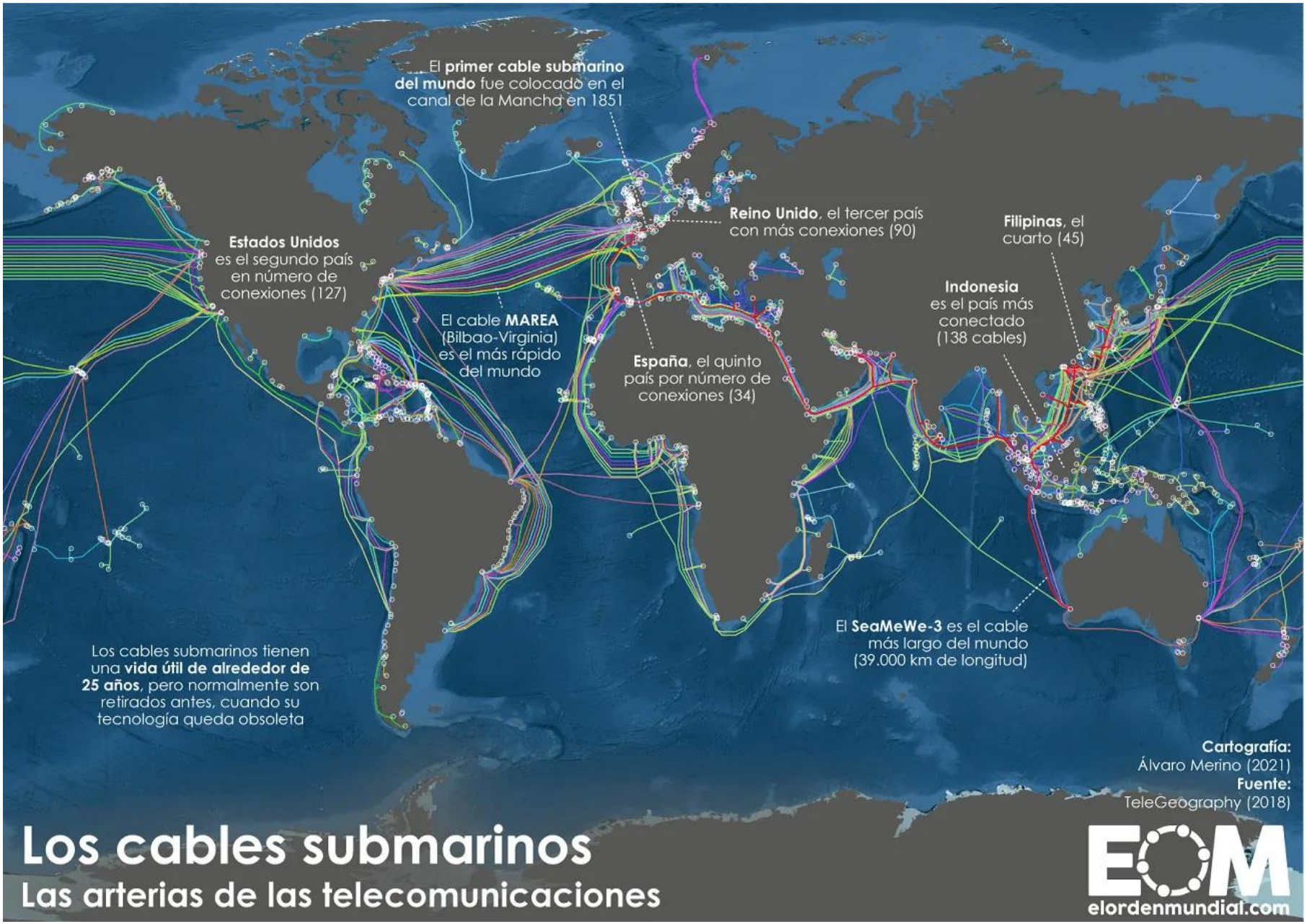
Arquitecturas de estas redes



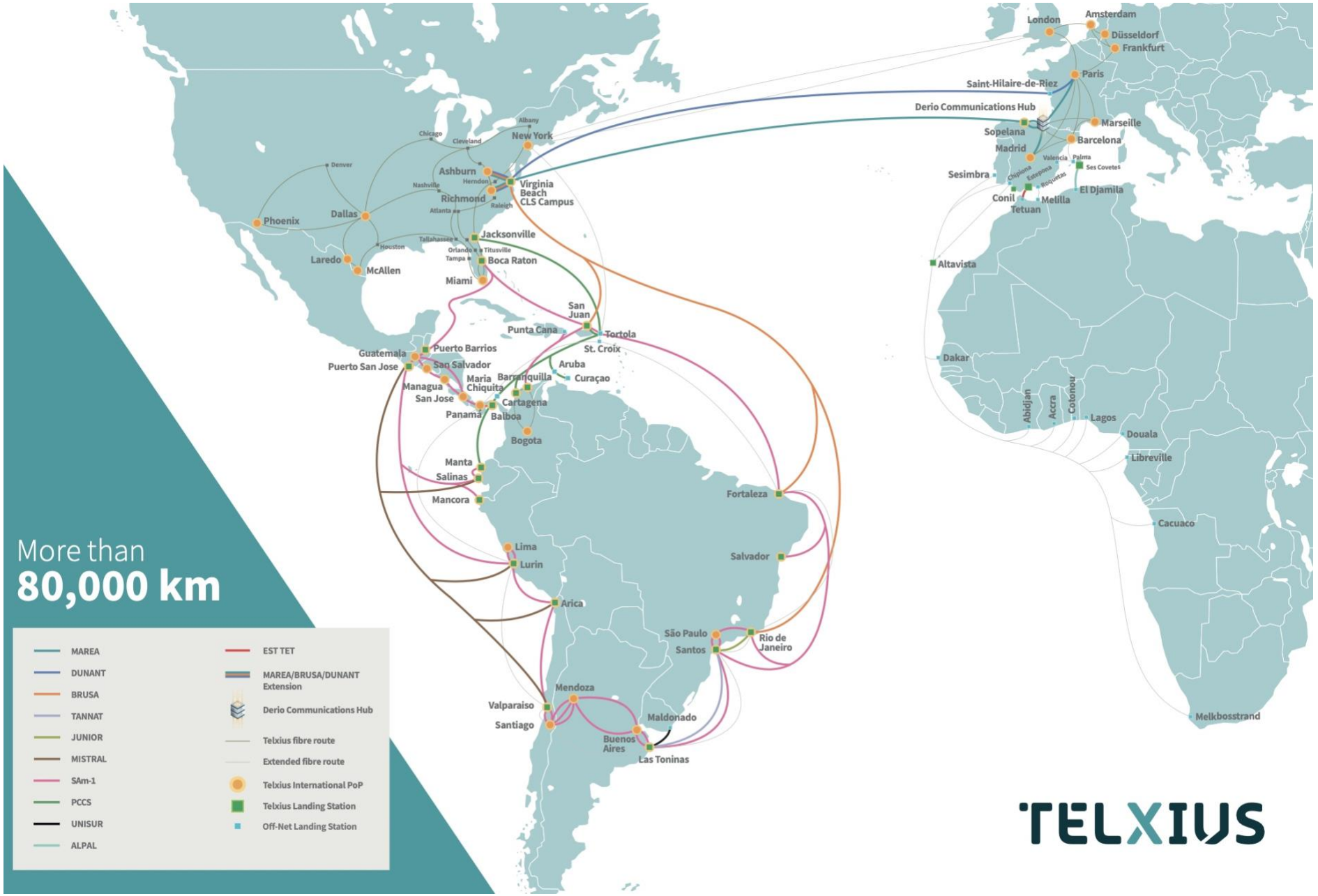
Jerarquía de estas redes.



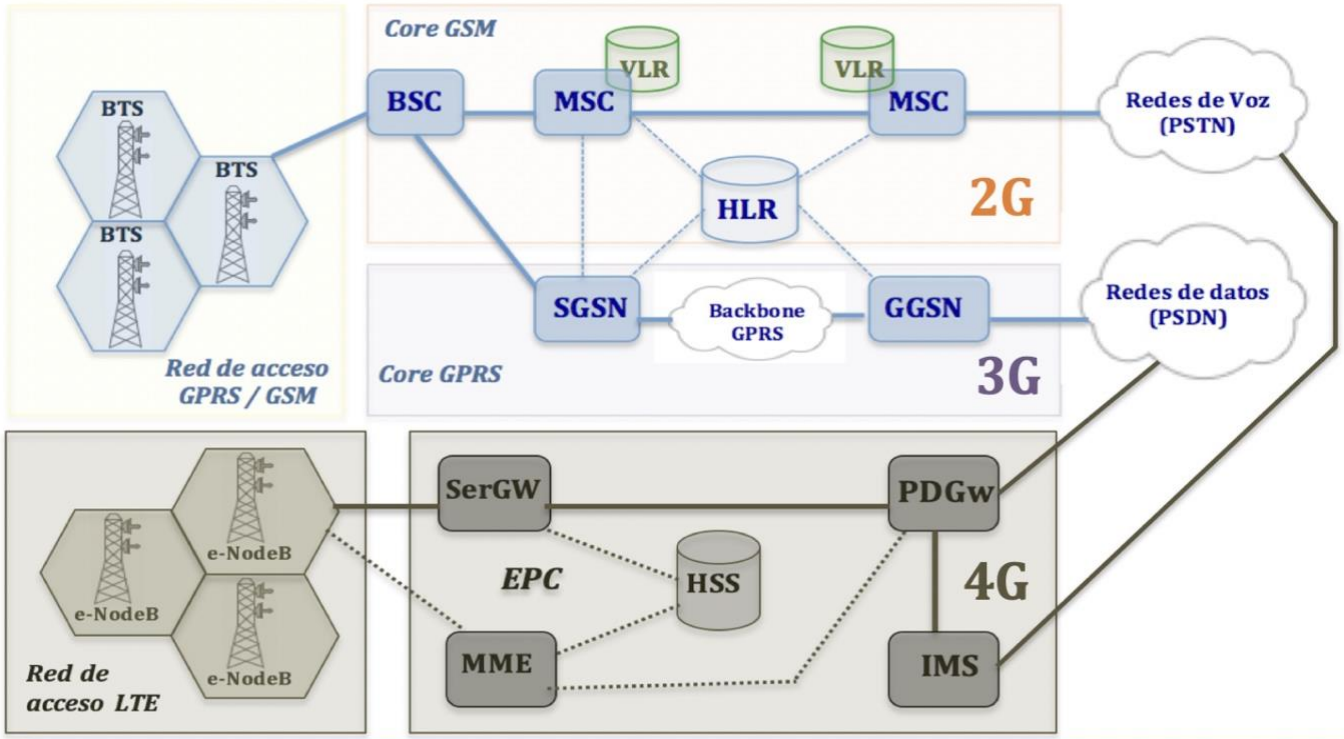
Fibra óptica en el mundo.

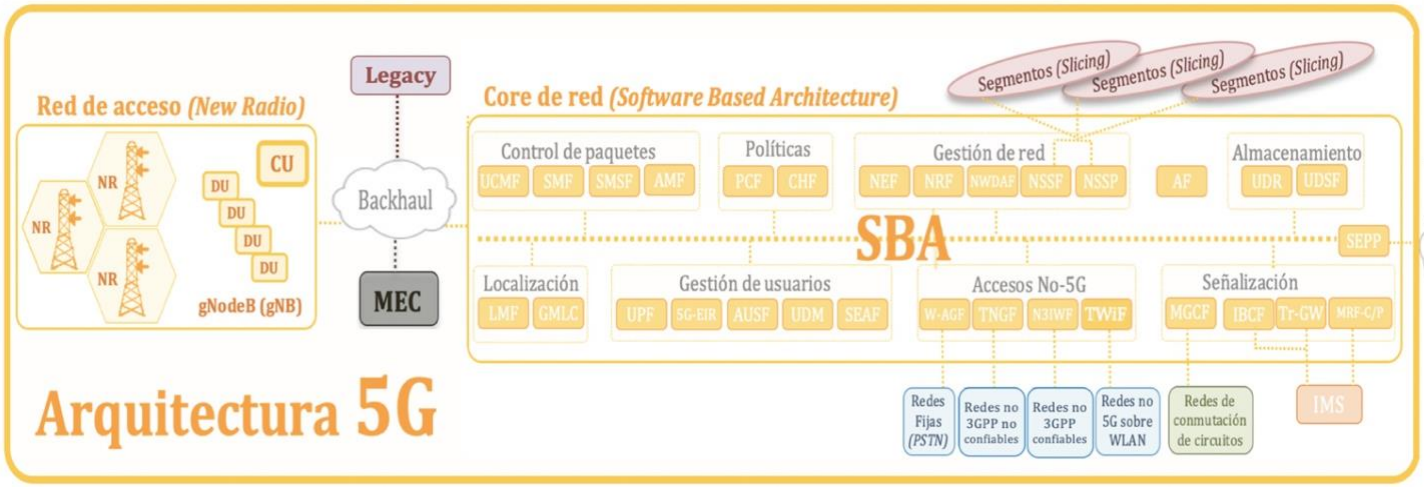


TELXIUS (Tier One del grupo Telefónica) - https://telxius.com/network/interactive-map/cables



Evolución de 2, 3, 4 a 5G (Presentación y evolución de las tecnologías móviles)





- **1G** (1979): primera generación de redes de telecomunicaciones , solo voz y cierta movilidad.
- **2G** (1991): nacen los SMSs y comienza el roaming.
- **3G** (1998): Comienzan los accesos a Internet con cierta calidad de servicio.
- **3.5G** (2006): Se afianza Internet - HSDPA (High Speed Downlink Packet Access).
- **4G** (2009): Servicios totalmente IP (voz y datos), aumenta considera-blemente el ancho de banda.
- **4G LTE** (2011): duplicó las velocidades de datos. Implantación de VoLTE.
- **5G** (2020): NR, accesos, NFV, SBA, MEC, Slicing, latencia, confiabilidad, seguridad, privacidad.
- **6G:** ... ¿2026? ...

“Manual de Resiliencia”

(Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)

Alejandro Corletti Estrada

(acorletti@DarFe.es - acorletti@hotmail.com)

www.darFe.es

www.darFe.es

Con los especiales aportes de:

General de División **Evergisto de Vergara**

Introducción

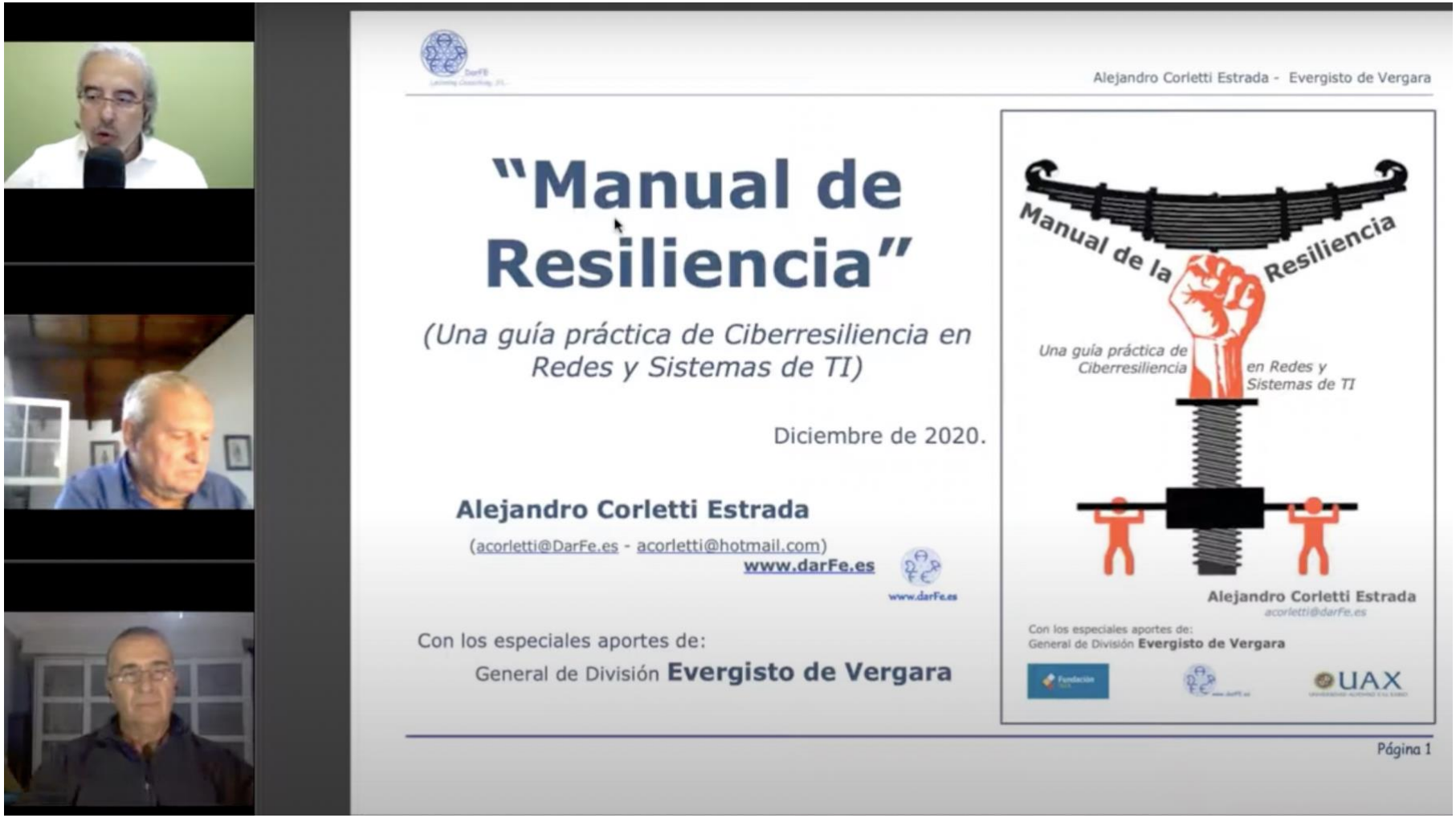
- Conceptos ya difundidos:
  - ➢ Defensa en profundidad y en altura.
  - ➢ Dinámica de la defensa.
  - ➢ De "Proteger y proceder" a "Seguir y perseguir" (RFC-1244)
  - ➢ Ciber operación de Acción retardante.
- Nuevos conceptos y desafíos:
  - ➢ Compartimentación de redes (la familia IEEE-802.x).
    - *Reducir superficie de ataque.*
    - *Arquitectura de red de confianza cero.*
    - *Organización por tecnologías.*
    - *Granularidad.*
    - *Exfiltración de datos.*
    - *Gestión de actualizaciones.*
    - *Capacidad de reacción.*
  - ➢ Ruido en la red.
  - ➢ Virtualización (de host y de redes).
  - ➢ Delegación y segregación de responsabilidades y funciones.
  - ➢ Contra inteligencia.
  - ➢ Juegos de ciberguerra.

*Hoy sumaremos a todos estos, el tema de la "**Resiliencia**" tratándola de forma detallada y desde sus diferentes puntos de vista, llegando a desarrollar una metodología o guía que nos pueda ser de utilidad desde el punto de vista técnico y para la operación del día a día en nuestras redes y sistemas de TI*

Las realidades inexistentes *(por el General de División* ***Evergisto de Vergara****).*

Presentación del libro **"Manual de la Resiliencia"** (parte 1)
https://youtu.be/vCeOmX4Ir80

Presentación del libro **"Manual de la Resiliencia"** (parte 2)
https://youtu.be/6GMa2eXNt24



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.

Las regulaciones.

El poder del siglo XXI se llama "**Información**".

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

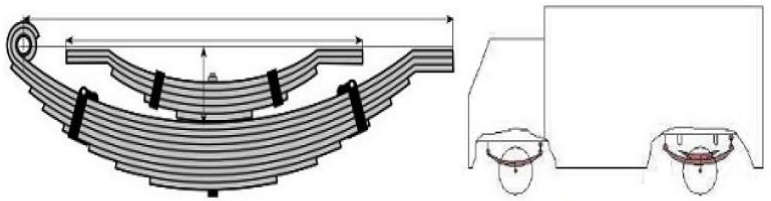
El tesoro es la "Información", no la infraestructura que la sustenta.

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

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

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.

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.

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**".*

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.

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

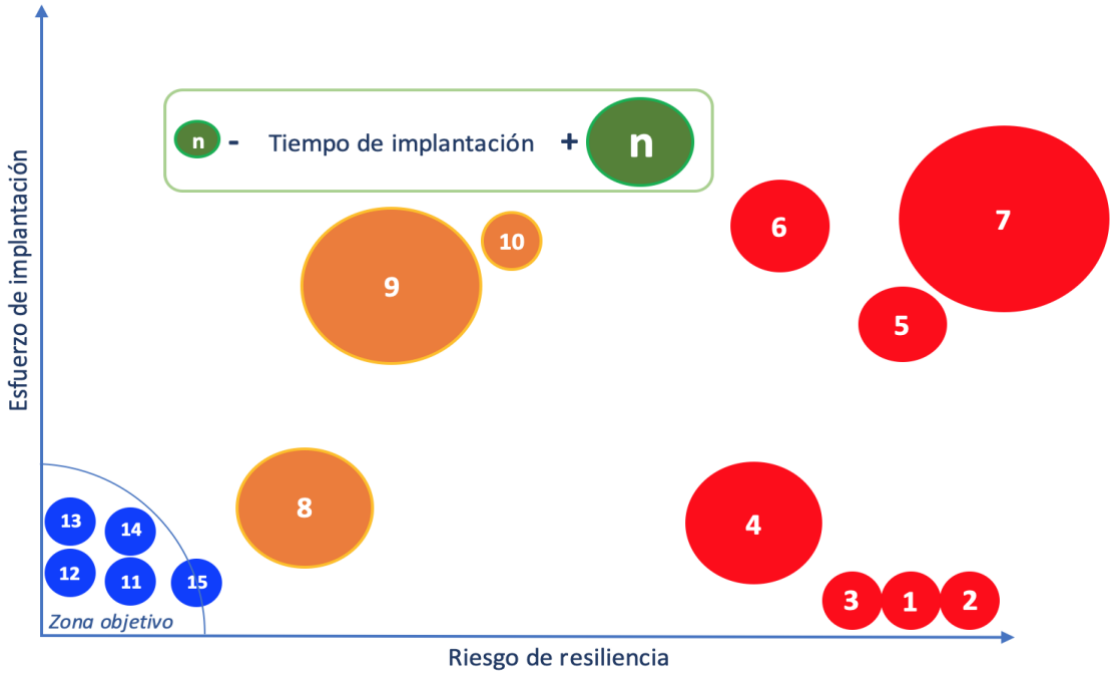
El objetivo fundamental de esta propuesta es avanzar en nuestra "**Matriz de Resiliencia**" tal cual lo propone la familia ISO/UNE 27000, paso a paso generemos un ciclo de mejora continua de la seguridad.

				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

Hagamos un análisis más de la plantilla recientemente presentada.

Estrategias Resilientes en Redes y Sistemas.

Para seguir avanzando ahora hacia nuestra estrategia de resiliencia, proponemos a continuación que se sigan haciendo valoraciones sobre los resultados obtenidos, esta vez nos centraremos en esfuerzos, tiempos y riesgos. Una vez más hemos asignado valores a estos conceptos, para que podemos desarrollar el tema de forma eminentemente práctica.



Lo primero que se pone de es la zona objetivo, allí se encuentran los aspectos positivos de nuestra evaluación, el ítem **(15)** se encuentra en la frontera de la misma (recordad que tenía "**8**" puntos

El tamaño de cada círculo representa el tiempo de implantación, los ejes "x" el riesgo desde el punto de vista de la resiliencia y el eje "y" el esfuerzo de implantación-

Cuanto más a la derecha del cuadro nos encontramos, mayor es el riesgo de, en este caso se tratarían de **(7)**, **(2)**, **(1)**, **(5)** y **(3)** en segundo orden podemos situar a **(4)** y **(6)**, y luego nos quedarían los tres color naranja, cuya calificación estaría por arriba de los "4" **(8)**, **(9)** y **(10)**.

Si prestamos atención al eje de las "**Y**" veremos que hay ítems que nos requerirán mayor esfuerzo de implantación, en este caso son **(7)**, **(6)**, **(10)**, **(9)** y **(5)**.

Por último, nos interesa analizar su tamaño en el cuadro que nos pone de manifiesto que los ítems **(7)**, y **(9)** nos requerirán más tiempo de implantación y en segundo orden estarían el **(8)** y el **(4)**.

Hemos logrado identificar en un cuadro de dos dimensiones, tres tipos diferentes de magnitudes que nos permitirán seguir adelante con nuestra "**estrategia de resiliencia**". Para poder ser aún mas detallistas, proponemos ponerles nombres

que sean representativos para nosotros y comenzar a evaluar un plan de acción para abordarlas. En nuestro caso, nuevamente lo haremos a través de una plantilla, que se presenta a continuación:

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)	

Estamos presentando un análisis temporal dos años de duración, dividido en cuatro semestres, y a su vez la plantilla nos muestra también su posible evolución mes a mes.

Hemos centrado la atención en los diez ítems que anteriormente identificamos con mayo riesgo:

(1) Determinación de RTO	**(5)** Obsolescencia BBDD y Backups	**(9)** DRP
(2) Determinación de RPO	**(6)** Mejoras en AntiDDoS	**(10)** SLAs
(3) Determinación de KPIs	**(7)** Reposición de grandes equipos	
(4) Mejoras en IDSs/IPSs	**(8)** Formación	

Cada uno de esos ítems son "**Actividades**" que debemos organizar cómo deseamos abordarlas. Es importante tener en cuenta que su "duración" ha sido considerada sobre la base del tamaño de cada uno de los círculos del cuadro anterior, es decir, la **(7)**, **(8)** y **(9)** duran 2 años, le sigue la **(4)** que dura solo un año, y los círculos más pequeños solo meses.

Las actividades que mayor riesgo tienen **(7)**, **(1)** y **(2)** se prevén lanzar de inmediato, luego las actividades **(3)**, **(5)** y **(6)**, planificadas desde el primer mes, su implantación real es a partir del mes 4. A partir de allí el resto. Los acuerdos de nivel de servicio (SLAs:**(10)**) nos hemos permitido "ajustar" su implantación a cuando mejor nos cuadre.

A la derecha se ve una zona **"gris"** que es la parte en que realizamos una primera aproximación de costes. Nuevamente, aquí lo hacemos basándonos en el cuadro y teniendo en cuenta el eje "Y" del mismo, pues cuanto más "alta" se encuentre la actividad, mayor esfuerzo de implantación requerirá (material y/o humano). Las actividades **(1)**, **(2)**, **(·3)** son las que económicamente menor coste tienen y, en este ejemplo en concreto, guardan relación no con gasto económico, sino con horas hombre de trabajo. En el extremo opuesto la actividad **(7)** es la más onerosa, seguidas de la **(6)**, **(10)**, **(9)** y **(5)**.

En la columna **"gris"** que sigue, vemos que nuevamente evaluamos la "**prioridad**". Este valor guarda relación con el riesgo que ya hemos puesto a cada una de ellas y su temporalidad. Esta nueva prioridad es uno de los valores que nos permitirá ir dándole forma a los diferentes cursos de acción que propondremos finalmente a la Dirección.

Por último se presentan las dos columnas **"grises"** que tienen por objetivo, distribuir estos costes estimados a lo largo de los dos años previstos.

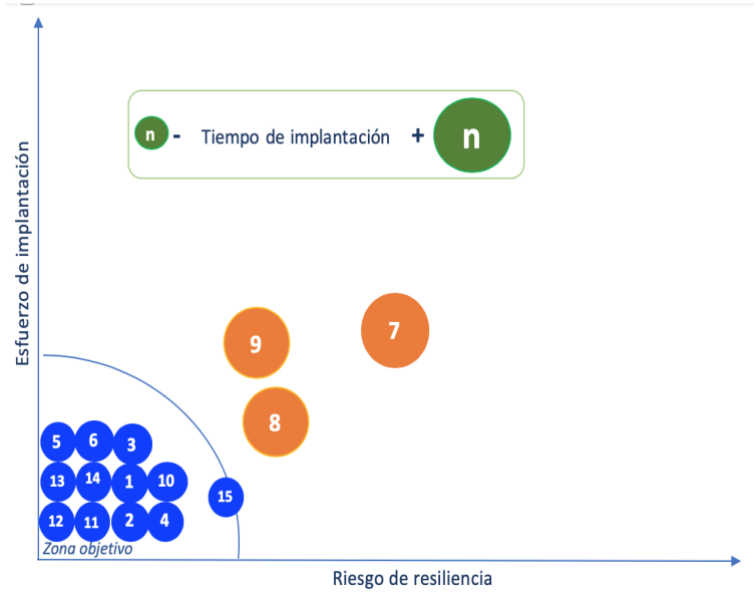
A continuación, presentamos, nuevamente a título de ejemplo, cómo podríamos definir estos cursos de acción.

a. Curso de acción "de máxima".

Este curso de acción, propone abordar el 100% de las acciones propuestas en los tiempos calculados, dando cumplimiento detallado a toda la planificación presentada en la plantilla inicial. El coste que implica para la empresa son **31.700 €** a pagar de la siguiente forma:

19.700 € + 4.500 € = 24.200 € el primer año - 7.500 € el segundo año

El resultado final de este curso de acción se verá reflejado de la siguiente forma:

A finales del primer año	A finales del segundo año
	

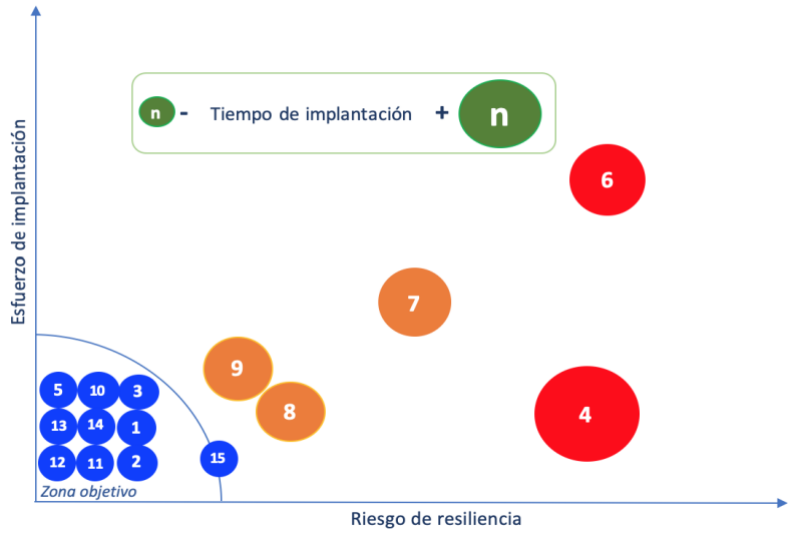
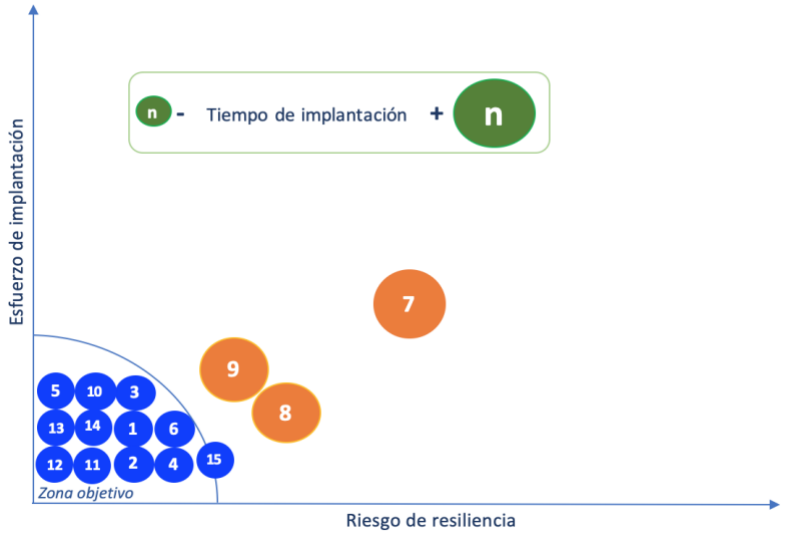
b. Curso de acción "intermedio".

Este curso de acción, propone abordar el **85%** de las acciones propuestas en los tiempos calculados, el coste que implica para la empresa son **24.200 €** a pagar de la siguiente forma:

17.700 € el primer año - **6.500 €** el segundo año

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			1ª 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 €	6.500 €

El resultado final de este curso de acción se verá reflejado de la siguiente forma:

A finales del primer año	A finales del segundo año
	

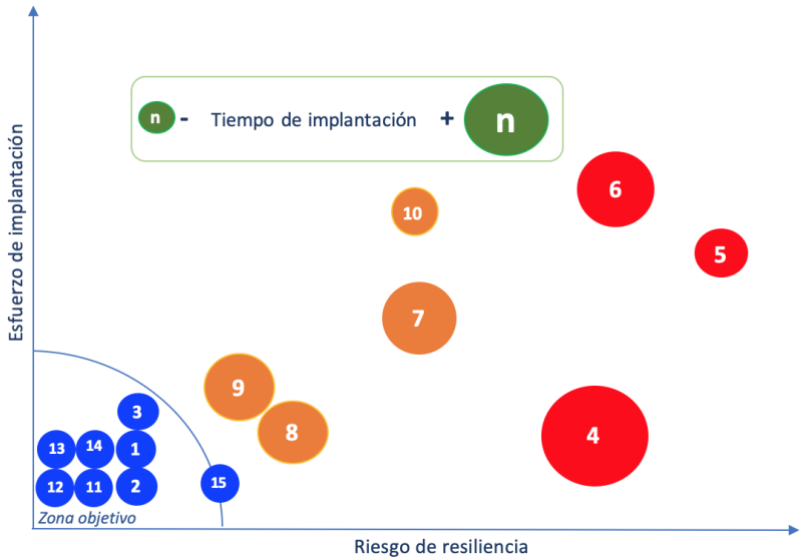
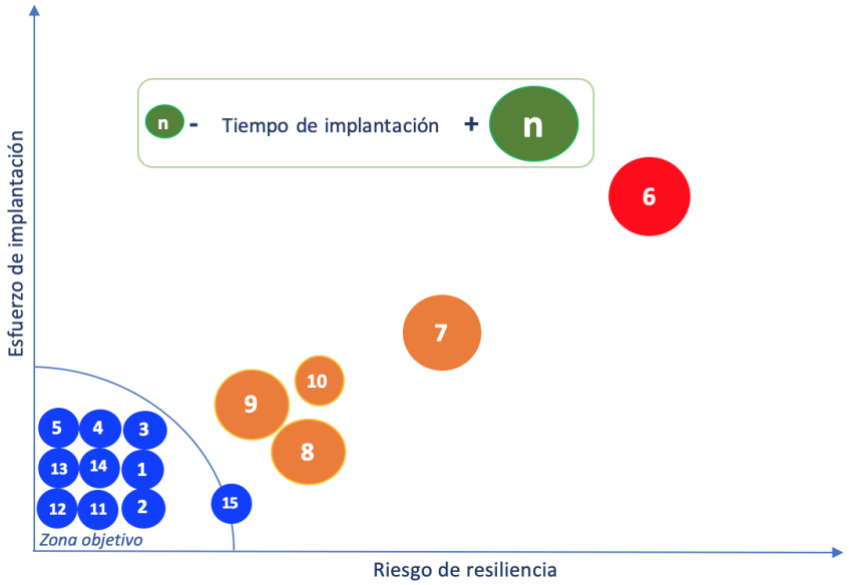
c. Curso de acción "de mínima".

Este curso de acción, propone abordar el **60%** de las acciones propuestas en los tiempos calculados, el coste que implica para la empresa son **16.700 €** a pagar de la siguiente forma:

9.200 € el primer año - **7.500 €** el segundo año

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 €	7.500 €

El resultado final de este curso de acción se verá reflejado de la siguiente forma:

A finales del primer año	A finales del segundo año
	

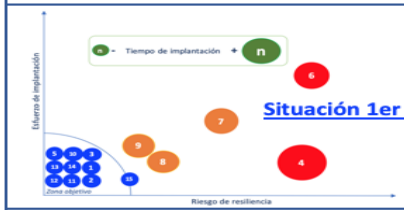
a. Curso de acción de máxima

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.

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

Muchas gracias