

“Manual de Resiliencia”

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

Diciembre de 2020.

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**



TEMARIO DEL DÍA DE HOY:

1. Introducción.
2. El poder de la Información y las realidades inexistentes.
3. Lo crítico es la "Información"... no las Infraestructuras.
4. Concepto físico de Resiliencia.
5. Introducción a redes y sistemas Resilientes.
6. Análisis de Riesgo de Resiliencia.
7. Matriz de Resiliencia.
8. Estrategias Resilientes en Redes y Sistemas.
9. Ciclo de Vida.
10. Procesos de ciberseguridad relacionados a Resiliencia.
11. Planes de formación y concienciación.
12. Normas y estándares técnicos a tener en cuenta sobre resiliencia

1. Introducción

⊗ Conceptos ya difundidos:

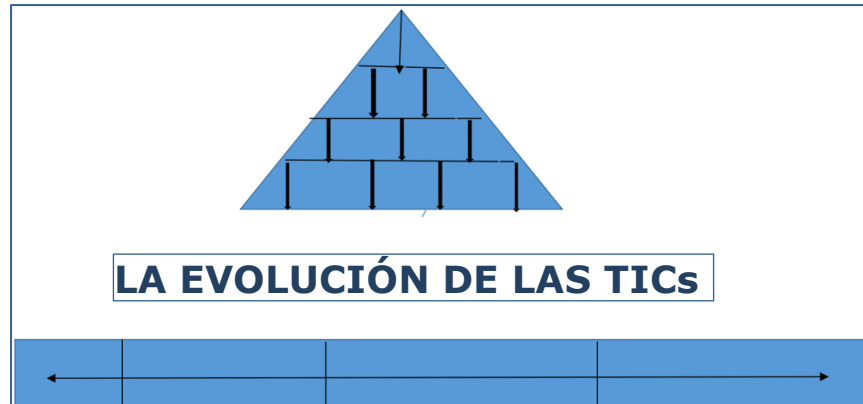
- Defensa en profundidad y en altura.
- Dinámica de la defensa.
- De "Proteger y proceder" a "Seguir y perseguir" (RFC-1244)
- Ciber operación de Acción retardante.

⊗ 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 ciber guerra.

*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*

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



TODO ES INFORMACIÓN

La **tecnología** ha permitido que medios significativos **interrumpan, manipulen, distorsionen y nieguen información**, tecnología que los adversarios han ya demostrado que tienen la voluntad de usar con gran efecto ...[...] **quien controle la información puede dominar la competencia y el conflicto.**

(Vertuli Mark, Loudon Bradley, 2018, pág. xii)

OPERACIONES DE INFORMACIÓN

Acciones tomadas por actores organizados (gobiernos o actores no estatales) **para distorsionar el sentimiento político nacional o extranjero**, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas destinadas a manipular la opinión pública (*nos referimos a estos como "amplificadores falsos"*).

NO SOLO BUSCA AFECTAR MILITARES

...SINO TAMBIÉN Y PRINCIPALMENTE A MÚLTIPLES AUDIENCIAS SIMULTÁNEAMENTE, AFECTANDO A ACTORES ESTATALES, SOCIEDADES E INDIVIDUOS NO SOLO EN EL TEATRO GEOGRÁFICO DEL CONFLICTO, SINO EN EL NIVEL MUNDIAL.

"Efectos simultáneos a toda la profundidad del territorio enemigo, en todo medio físico de comunicación y en el dominio de la información."

Valeriy Gerasimov

Esta nueva Guerra Fría se diferencia de la anterior en que vivimos en un mundo globalizado. Así pues, los medios de comunicación e Internet, es decir, la construcción narrativa del conflicto, se convierten en un elemento fundamental.

Jesús M. Perez Triana, Las Guerras Posmodernas

CAMPAÑAS DE INFORMACIÓN

DAR IDEA DE CONSENSOS Y OPINIONES PÚBLICAS GENERALIZADAS, PARA ESGRIMIR CLAMORES POPULARES Y PODER HACER LO QUE SE DESEE PARA LLEGAR, EJERCER Y MANTENERSE EN EL PODER.

LAS REALIDADES INEXISTENTES

- *La Disinformation*
- *La Misinformation*
- *La Manipulación*

HAY QUE LLEVAR A CABO LA LUCHA
POR LA OPINIÓN PÚBLICA COMO SE
ESTUVIERA LIBRANDO UNA GUERRA



**El riesgo más grande es que la desinformación,
la manipulación y las redes sociales venzan el
espíritu de resistencia de los hombres y las
naciones haciéndoles ver como favorables a
situaciones que van en contra de sus intereses
legítimos, y su bienestar.**

ES EL PODER DE LA INFORMACIÓN.



3. 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).



Analicemos la situación desde el punto de vista de la Unión Europea (**UE**).

En junio de **2004**, el Consejo Europeo solicitó la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas.

El 17 de noviembre de **2005**, la Comisión adoptó el **Libro Verde** sobre un Programa Europeo para la Protección de Infraestructuras Críticas.

En diciembre de **2005**, el Consejo de Justicia y Asuntos de Interior pidió a la Comisión que elaborara una propuesta para un programa europeo de protección de las infraestructuras críticas (el **PEPIC**).

El 8 de diciembre de **2008** se publica la Directiva **2008/114/CE** del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

En su artículo 2 Definiciones, expresa:

A efectos de la presente Directiva, se entenderá por:

- a) *«**infraestructura crítica**», el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;*
- b) *«infraestructura crítica europea» o «ICE»... idem situada en los Estados miembros.*

En España, siguiendo esta línea de la UE, se publica la **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

No merece la pena seguir detallando normativas, la intención de los párrafos anteriores era solamente presentar la secuencia de cómo se fue avanzando en Europa sobre el tema de Ciberdefensa y remarcar que el concepto base de todo esto fue siempre "**Infraestructuras críticas**", concepto que no comparto del todo.

Sin embargo, hasta la misma administración española, en este aspecto presenta una cierta incoherencia, pues como veremos más adelante, la metodología de análisis de riesgo **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) en su punto 2.1 "Activos esenciales" expone:

En un sistema de información hay 2 cosas esenciales:

- ✓ *la **información** que se maneja y*
- ✓ *los **servicios** que prestan.*

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema".

3.1. 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*) \implies (Nuevo concepto: "**Crowdwarefare**").

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.

3.3. La raíz del problema.

Cuando se unen:

- **el tiempo milenario.**

y

- **la experiencia muy afianzada.**

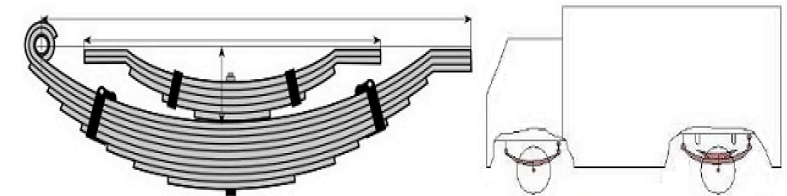
*Las empresas líderes del mercado apuestan por el "poder de la Información". En estos momentos Google, Facebook, Whatsapp, apuestan por tener más y más "**Información**" que le permitan inferir o inducir tendencias (sexto escenario: "Opinión").*

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

4. 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"

5. 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.

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 de todo lo que hace. Cuánto más preciso sea en la definición de esos límites mayor será su capacidad ejecutiva. Todas las fases de un proyecto requerirán este tipo de decisiones, y no sólo en el ámbito de ingeniería, sino más bien en la vida misma. En el ámbito empresarial, se traduce en la relación **coste/beneficio** de estas decisiones, y ese balance óptimo hace ahorrar mucho dinero, tiempo, esfuerzos y dolores de cabeza.

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).

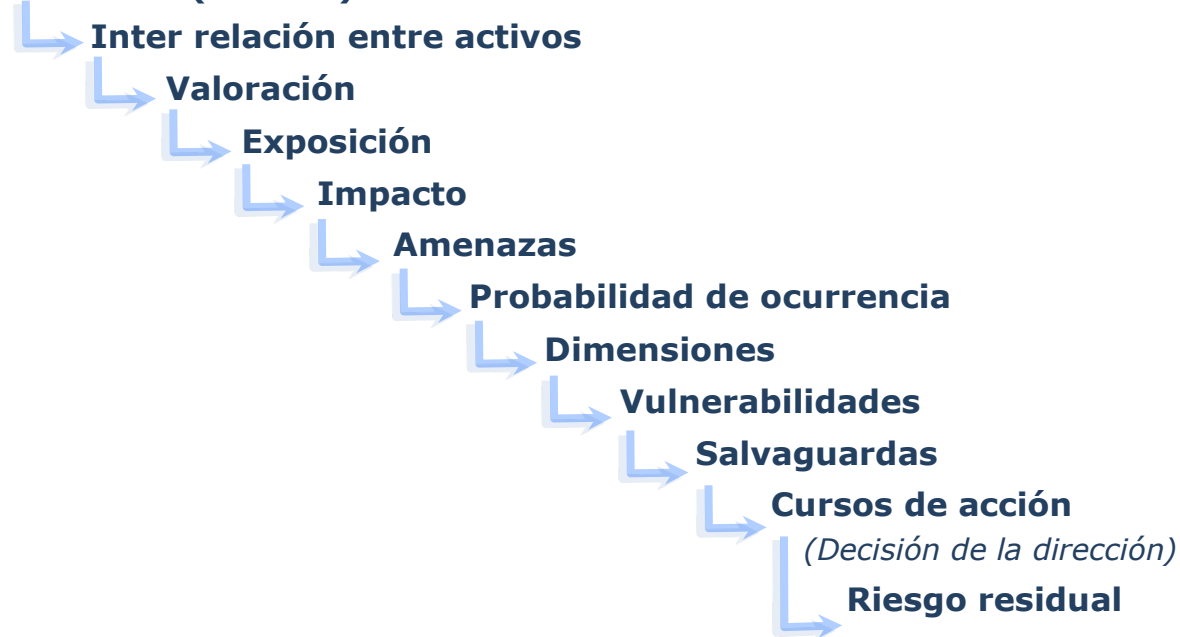
6. Análisis de Riesgo de Resiliencia.

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)



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

"Análisis de Riesgo de Resiliencia".

¿Por qué razón se ha decidido llamarlo así?

Creo que lo que mejor define este título lo hemos basado en un artículo muy interesante publicado en:

http://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf, cuyo título es "**Conceptualizing and Measuring Resilience**" A Key to Disaster Loss Reduction (Escrito por **K. Tierney** y **M. Bruneau**).

Esta publicación se refiere a desastres naturales y hace un análisis que merece la pena ser leído, pero lo que deseábamos destacar es que nos pareció muy interesante esta visión que hace de lo que en inglés define como "**4R**": robustness, redundancy, resourcefulness, and rapidity.

En español, lo traduciríamos como: robustez, redundancia, inventiva (ingenio) y rapidez.

- **Robustez**: la capacidad de los sistemas, elementos del sistema y otras unidades de análisis para resistir las fuerzas del desastre sin una degradación significativa o pérdida de rendimiento.
- **Redundancia**: la medida en que los sistemas, elementos del sistema u otras unidades son sustituibles, es decir, capaces de satisfacer los requisitos funcionales, si se produce una degradación o pérdida significativa de la funcionalidad.
- **Inventiva** (ingenio): la capacidad de diagnosticar y priorizar problemas e iniciar soluciones mediante la identificación y movilización de recursos materiales, monetarios, informativos, tecnológicos y humanos.
- **Rapidez**: la capacidad de restaurar la funcionalidad de manera oportuna, conteniendo pérdidas y evitando interrupciones.

7. 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:

<u>Objetivos y gestión</u>	<u>Ciclo de vida</u>	<u>Arquitectura de ciberdefensa</u>
<p><u>Reflexión 4</u>: Resiliente a qué.</p> <p><u>Reflexión 5</u>: Amortiguación (rebote).</p> <ul style="list-style-type: none"> • Gobierno de la Ciberseguridad. • Gestión de riesgos. • Gestión de incidencias. • Plan de recuperación de desastres <p><u>Reflexión 7</u>: Esfuerzo de mantenimiento.</p> <ul style="list-style-type: none"> • Tipo de soporte. • precio del soporte. • SLAs 	<p><u>Reflexión 1</u>: Límite (umbral) elástico, plástico o de rotura.</p> <ul style="list-style-type: none"> • Entorno del activo. • Ciclos de trabajo. • Obsolescencia. • Redundancia. <p><u>Reflexión 6</u>: Tiempo de respuesta óptimo.</p> <ul style="list-style-type: none"> • Gestión de copias de respaldo y recuperación. • RTO (Restoration Time Objective). • RPO (Restoration Point Objective). <p><u>Reflexión 8</u>: Fisuras (o degradación).</p> <ul style="list-style-type: none"> • Parcheado. • Actualizaciones. • Formación <p><u>Reflexión 9</u>: Grado de deformación.</p> <ul style="list-style-type: none"> • KPI - Indicadores Clave de Desempeño 	<p><u>Reflexión 2</u>: Equilibrio entre rigidez y flexibilidad.</p> <ul style="list-style-type: none"> • Defensa en profundidad. <p><u>Reflexión 3</u>: Calidad del material (no necesariamente precio).</p> <ul style="list-style-type: none"> • Diseño. • Seguridad del software. • Componentes. <p><u>Reflexión 10</u>: Presiones persistentes.</p> <ul style="list-style-type: none"> • 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.

Nº	Activos críticos	Valoración	Reponible	Objetivos y gestión								Ciclo de vida										Arquitectura de ciberdefensa					
				Resiliente a qué	Gobierno de la Ciberseguridad	Gestión de riesgos	Gestión de incidencias	Plan de recuperación de desastres	Tipo de soporte	precio del soporte	SLAs	Entorno del activo	Ciclos de trabajo	Obsolescencia	Redundancia	RTO	RPO	Parcheado	actualizaciones	formación	KPI	Defensa en profundidad.	Seguridad del software	Componentes	FWs	AntiDDoS	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

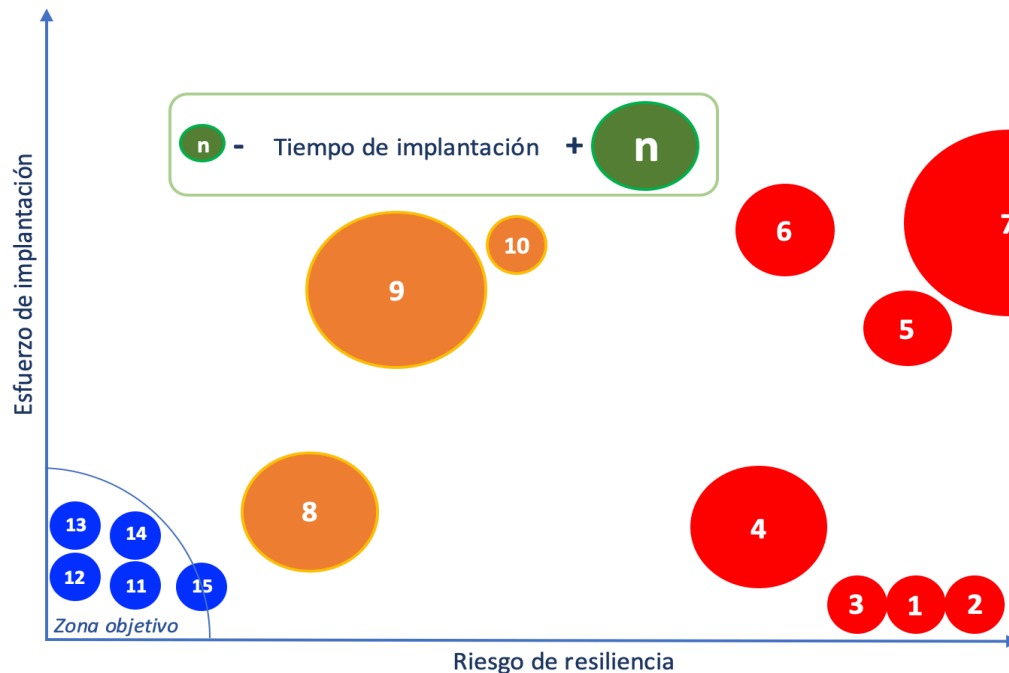
El objetivo fundamental de esta propuesta es avanzar en nuestra "Matriz de Resiliencia" tal cual lo propone la familia ISO/UNE 27000, paso a paso generemos un ciclo de mejora continua de la seguridad.

Nº	Activos críticos	Valoración	Reponible	Objetivos y gestión								Ciclo de vida										Arquitectura de ciberdefensa					
				Resiliente a qué	Gobierno de la Ciberseguridad	Gestión de riesgos	Gestión de incidencias	Plan de recuperación de desastres	Tipo de soporte	precio del soporte	SLAs	Entorno del activo	Ciclos de trabajo	Obsolescencia	Redundancia	RTO	RPO	Parcheado	actualizaciones	formación	KPI	Defensa en profundidad.	Seguridad del software	Componentes	FWs	AntiDDoS	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.

8. 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	AÑO1												AÑO2												Presu- puesto	Prio- ridad	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.

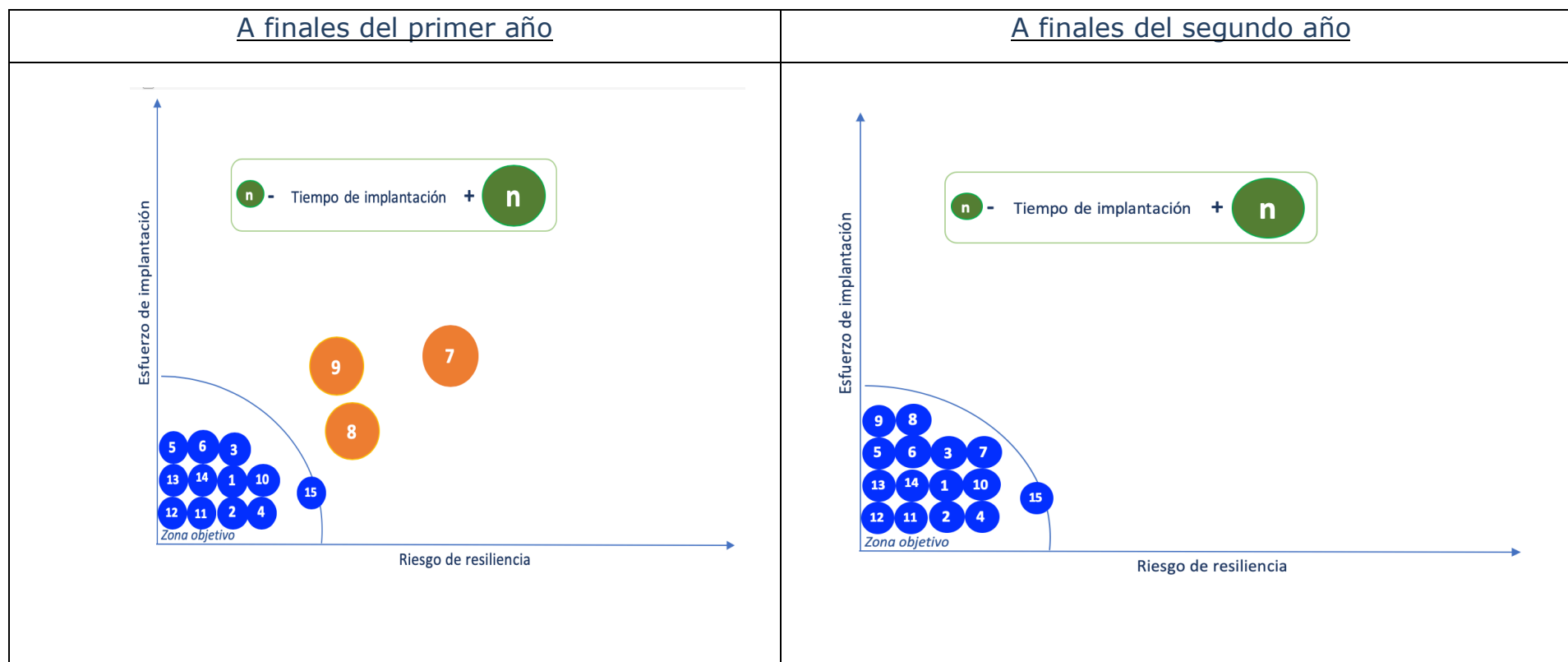
A continuación, presentamos, nuevamente a título de ejemplo, cómo podríamos definir estos cursos de acción.

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:



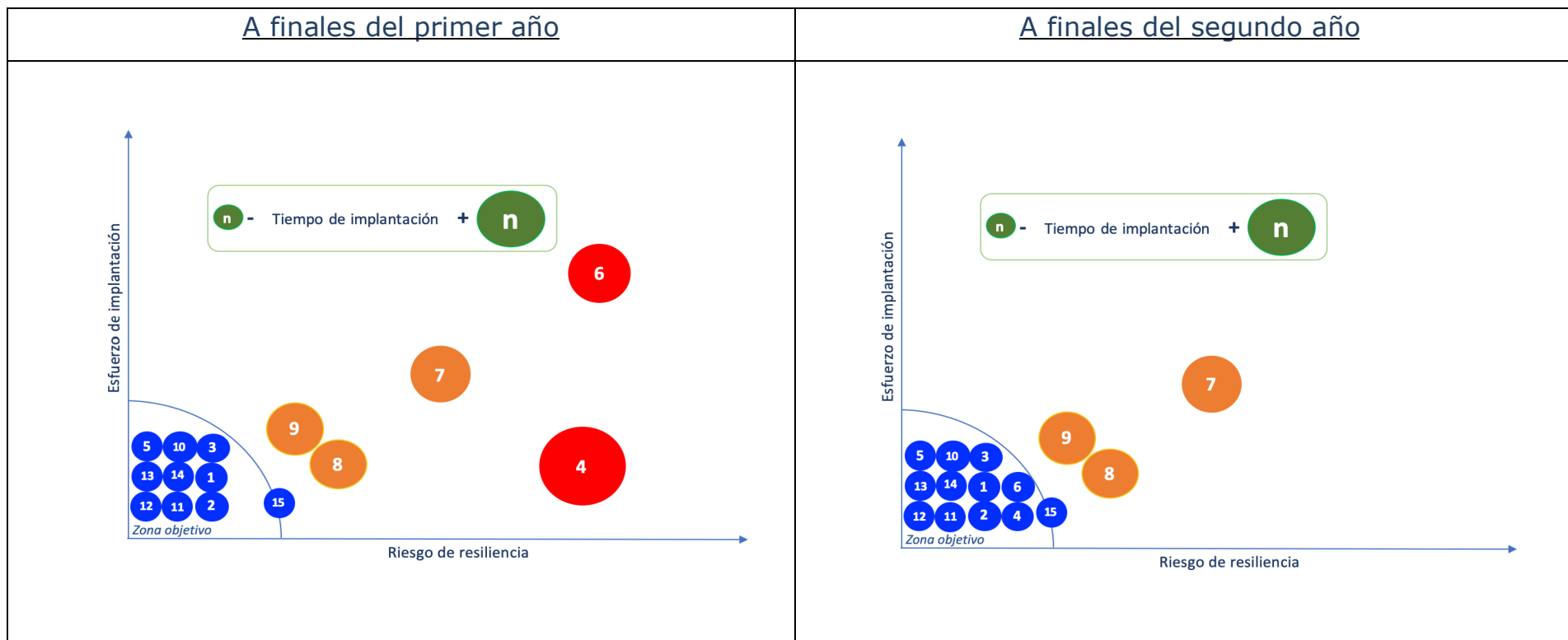
b. Curso de acción "intermedio".

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

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

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año						
		1er. Semestre				2do. Semestre				3er. Semestre				4to. Semestre																					
(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)																								4.500 €	1	1º año	
(8)	Formación	Plan formación		Fase 1		Med. Resultados																								800 €	5	2º Sem			
(9)	DRP	Análisis		Fase 1		Pruebas																								2.200 €	5	2º Sem			
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año							
																										24.200 €		17.700 €	6.500 €						



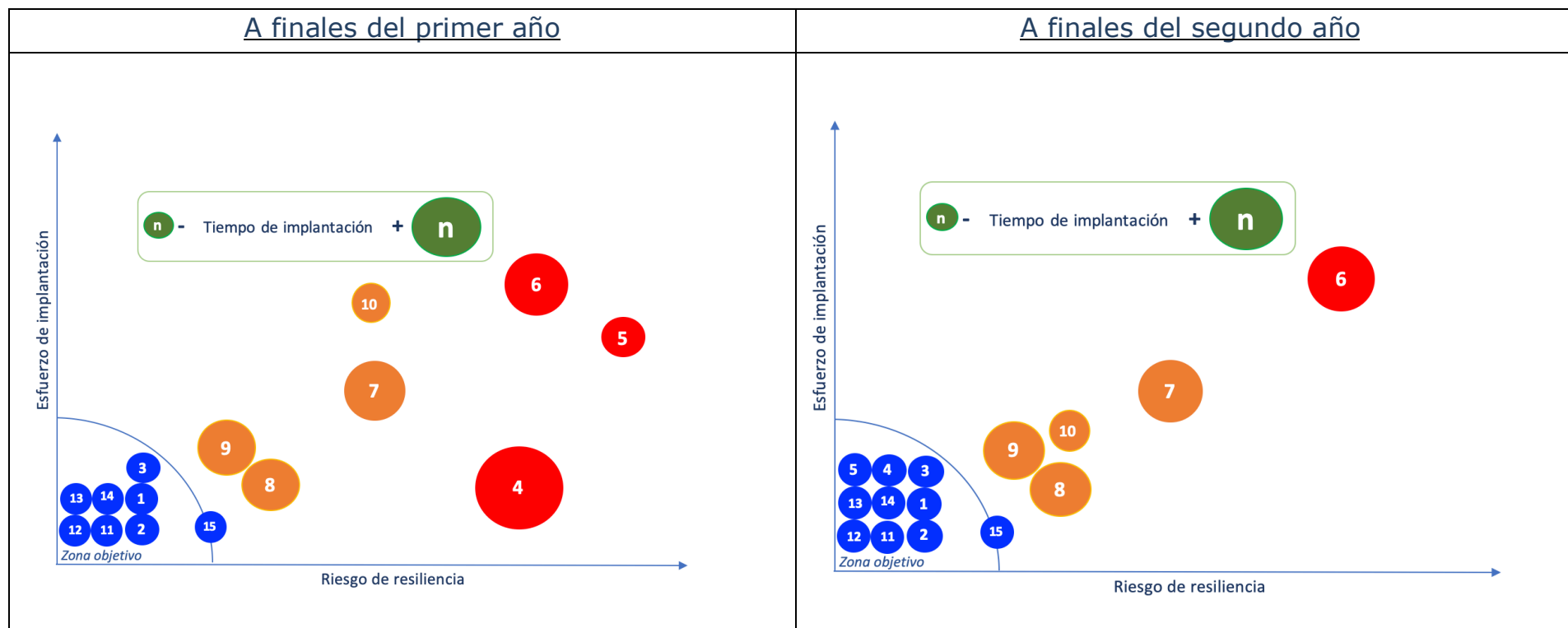
c. Curso de acción "de mínima".

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:

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
(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 LLEVARÁ A CABO								4.500 €	1	1º año				
(8)	Formación			Plan formación		Fase 1		Med. Resultados		NO SE LLEVARÁ A CABO								800 €	5	2º Sem						
(9)	DRP			Análisis		Fase 1		Pruebas		NO SE LLEVARÁ A CABO								2.200 €	5	2º Sem						
(10)	SLAs													Firma de nuevos contratos (con mínimos SLAs)								2.000 €	4		2º año	
																						16.700 €			9.200 €	7.500 €

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

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



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

“Estrategia de Resiliencia” que adoptaremos para los próximos dos años.

a. Curso de acción de máxima

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prio-ridad	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						
(5)	Obsolescencia BBDD y Backups	Implementación																								4.000 €	2	1º Sem					
(6)	Mejoras en AntiDDoS	Análisis/presupuestos																								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	Análisis/presupuestos																								1.500 €	5	2º Sem	2º año				
(9)	DRP	Análisis																								4.500 €	5	2º Sem	2º año				
(10)	SLAs	Fase 1																								4.500 €	4	Ajustable					
		←- 1 mes →- (desplazable según presupuesto y costes)																								31.700 €			19.700 €	7.500 €	4.500 € (ajustable)		

Situación 1er año

Situación 2do año

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	Prio-ridad	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	Implementación																								4.000 €	2	1º Sem					
(6)	Mejoras en AntiDDoS	Análisis/presupuestos																								5.000 €	3		2º año				
(7)	Reposición de grandes equipos	Análisis/presupuestos		Plan migración		1ra. Compra/despliegue		Entrada producción (1ra compra)		Análisis/presupuestos		Pruebas		Implementación		NO SE LLEVARÍA A CABO						4.500 €	1	1º año									
(8)	Formación	Análisis/presupuestos																								800 €	5	2º Sem					
(9)	DRP	Análisis																								2.200 €	5	2º Sem					
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año					
																										24.200 €			17.700 €	6.500 €			

Situación 1er año

Situación 2do año

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	Prio-ridad	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	Implementación																								4.000 €	2		2º año				
(6)	Mejoras en AntiDDoS	Análisis/presupuestos																								5.000 €	3						
(7)	Reposición de grandes equipos	Análisis/presupuestos		Plan migración		1ra. Compra/despliegue		Entrada producción (1ra compra)		Análisis/presupuestos		Pruebas		Implementación		NO SE LLEVARÍA A CABO						4.500 €	1	1º año									
(8)	Formación	Análisis/presupuestos																								800 €	5	2º Sem					
(9)	DRP	Análisis																								2.200 €	5	2º Sem					
(10)	SLAs	Firma de nuevos contratos (con mínimos SLAs)																								2.000 €	4		2º año				
																										16.700 €			9.200 €	7.500 €			

Situación 1er año

Situación 2do año

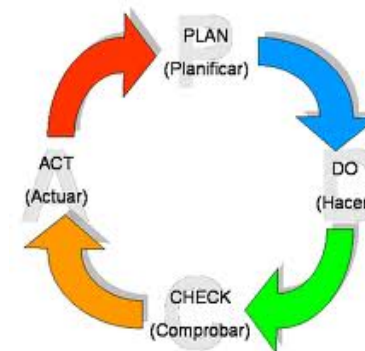
Coste 16.700 €
a pagar:
9.200 € el primer año
7.500 € el segundo año
se aborda el 60% de las acciones

9. Ciclo de Vida.

Para seguir manteniendo como referencia los estándares internacionales, este punto lo basaremos en la familia **ISO/UNE 27000**.

PLAN	Establecer SGSI.	Definir las métricas.
DO	Implementar y Operar el SGSI.	Implantar las métricas.
CHECK	Supervisar y Revisar el SGSI.	Revisar los datos de las métricas.
ACT	Mantener y Mejorar el SGSI.	Revisar/Mejorar las métricas.

Este estándar internacional adopta también el modelo "Plan-Do-Check-Act" (**PDCA**),



"Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información".

Los puntos: 6 Planificación, 6.1 Acciones para tratar los riesgos y oportunidades, 6.1.1 Consideraciones generales

- a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;
- b) prevenir o reducir efectos indeseados; y
- c) lograr la mejora continua.

La organización debe planificar:

- d) *las acciones para tratar estos riesgos y oportunidades;* y
- e) *la manera de:*

- 1) *integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información,*
y
- 2) *evaluar la eficacia de estas acciones.*

En el punto: 9 Evaluación del desempeño, 9.1 Seguimiento, medición, análisis y evaluación:

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

- a) a qué es necesario hacer seguimiento y qué es necesario medir*
- b) los métodos de seguimiento, medición, análisis y evaluación*

Para comprender y ejecutar estas métricas, nuevamente nada mejor que basarnos una vez más en estándares, así que seguiremos adelante en este capítulo, ahora con la norma **ISO/IEC 27004**.

Cabe mencionar que existen dos estándares más que se pueden tener en cuenta para la implementación de métricas de seguridad, estos son del **NIST** (National Institute of Standards and Technology), el **NIST 800-55** "Security Metrics Guide for Information Technology Systems" y el **NIST 800-80** "Guide for Developing Performance Metrics for Information Security".

10.1. Presentación del estándar ISO/IEC 27004 (diciembre de 2009 y su última revisión fue en año 2016).

Como venimos intentando remarcar, uno de los aspectos mas importantes que se debe destacar del estándar ISO 27001, es la importancia que hace sobre el carácter "medible de los controles

¿cómo debemos medir esos controles?

Atributo: Propiedad o característica de una "entidad".

Entidad: Un objeto (tangibles o intangibles)

Indicador: Es una medida que provee una estimación o evaluación de un "atributo"

Existen dos tipos de métodos para cuantificar los atributos:

- Subjetivos: Implica el criterio humano.
- Objetivos: Se basan en una regla numérica, puede ser aplicada por personas o recursos automatizados.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos.

- Encuestas/indagaciones.
- Observación.
- Cuestionarios.

www.darFe.es:

Descargas -> Tecnologías de la Información
-> Ciberseguridad -> ISO 27000

- Valoración de conocimientos.
- Inspecciones.
- Re-ejecuciones.
- Consulta a sistemas.
- Monitorización (“Testing”)
- Muestreo.

Un tema a considerar es la asociación de mediciones con determinadas escalas, de las cuales se proponen los siguientes tipos:

- Nominal: Los valores son categóricos.
- Ordinal: Los valores son ordenados.
- Intervalos: Se poseen máximos y mínimos con distancias entre ellos.
- Ratio: Tienen escalas de distancias, relacionadas a mediciones.

El último aspecto a considerar aquí es el de la **frecuencia**. Se deberían definir y programar claramente los intervalos en los cuales se llevará a cabo cada medición (Semanal, mensual, trimestral, anual, etc.).

Mejoras de las mediciones del SGSI (Fases Check y Act: monitorizar/auditar y actuar).

Las fases “**Check**” y “**Act**” facilitarán las mejoras y reencauces de los procesos de medición, y permitirán el análisis de la información de mediciones disponibles y su apoyo para la toma de decisiones

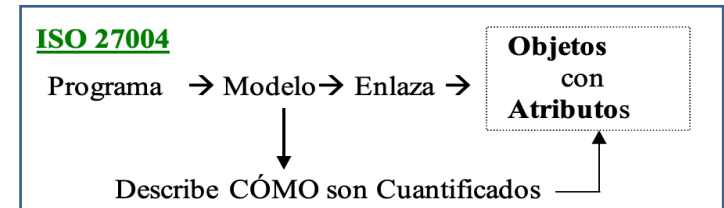
Este punto presenta dos aspectos:

- 1) Definir un criterio para evaluar la información (Análisis de información).
- 2) Definir un criterio para evaluar el proceso de mediciones (Validación de mediciones).

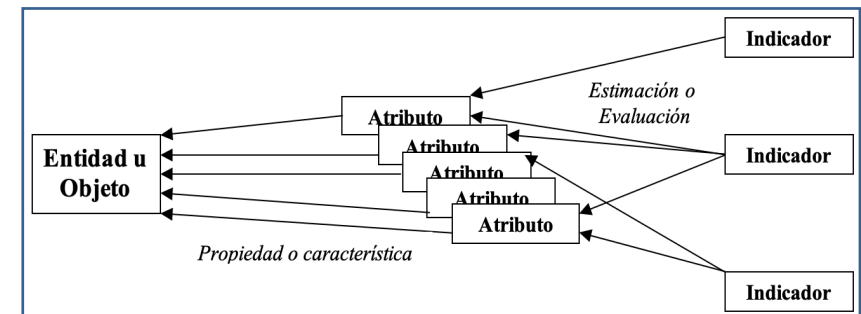
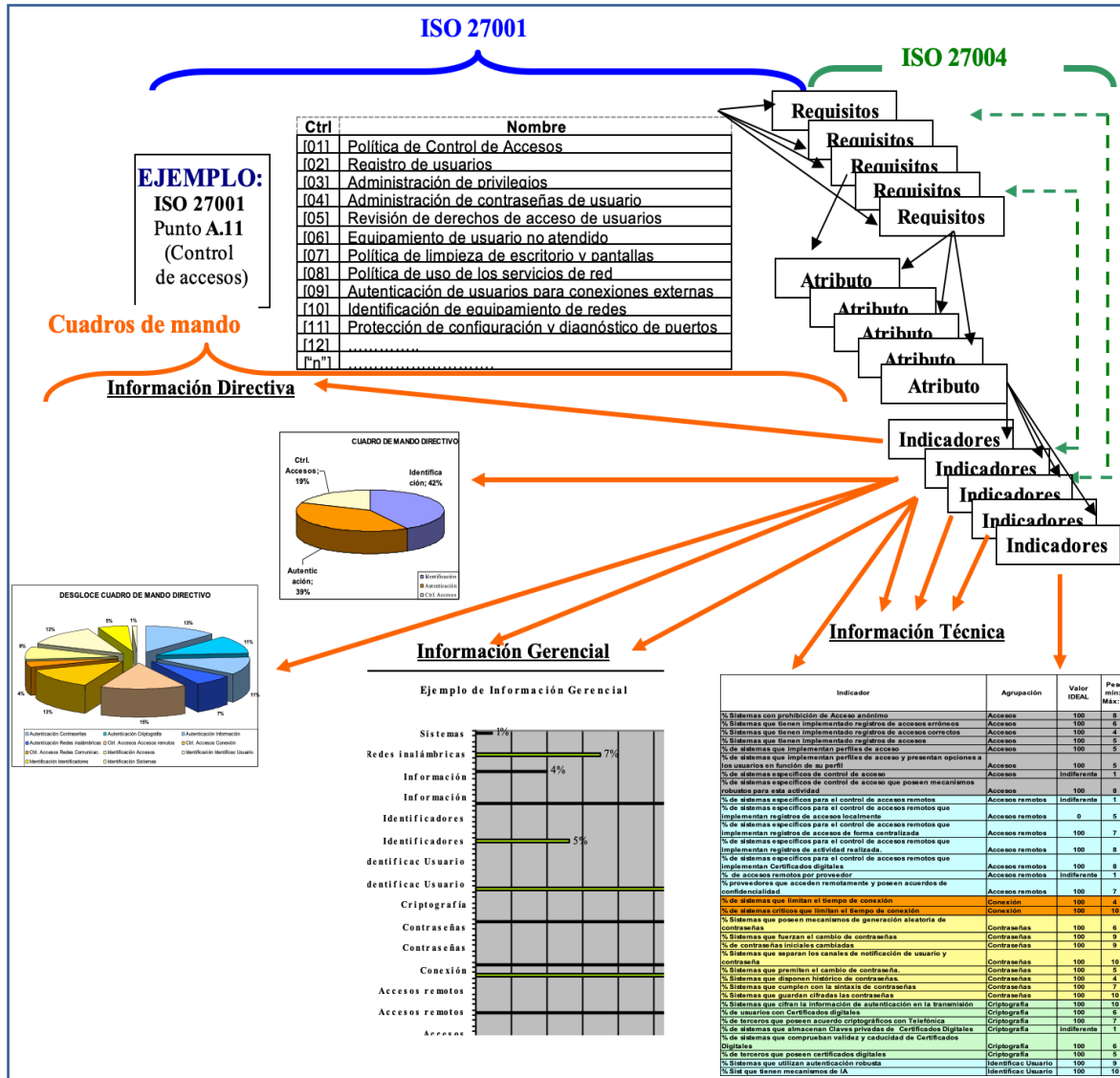
Las mediciones deberían ser revisadas, cuando ocurran cambios en la organización y también a intervalos planeados, para verificar si se siguen ejecutando tal cual se diseñó en su momento. El propósito de estas revisiones es asegurar que:

- Las mediciones son correctamente revisadas al ocurrir cambios en los objetivos de negocio.
- Las mediciones que no se suelen emplear son quitadas e ingresan nuevas mediciones necesarias.
- Los recursos que soportan estas mediciones son los adecuados.
- Las decisiones sean documentadas para permitir futuras comparaciones, o analizar tendencias.

Como se fue desarrollando, esta norma nos describe cómo cuantificamos "**Objetos**" con sus respectivos "**Atributos**".



Por lo tanto, si tenemos bien definidos los "**Controles**", si luego en el "**Análisis de riesgo**" identificamos cuáles son los "**activos críticos**". Si a cada uno de ellos los evaluamos respecto al nivel de "**Resiliencia**" que poseen, ahora podemos establecer el sistema de "**Medición**" y generar con ello un "**Cuadro de Mando**" que nos permita ejecutar con precisión ese ciclo "**Plan - Do - Check - Act**", siguiendo y manteniendo "**Viva**" nuestra **Estrategia de Resiliencia**.



10. Procesos de ciberseguridad relacionados a Resiliencia.

El **Centro Criptológico 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

Diciembre de 2020