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

"Una vida sin planes, está a la deriva" (A. Corletti)

Según la RAE, un **plan** es un modelo sistemático de una actuación pública o privada, que se elabora anticipadamente para dirigirla y encauzarla.

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

CMMC	Sigla	ISO 27002	Esquema Nacional de Seguridad	Sigla
Control de acceso	(CA)	A.9 Control de acceso	CONTROL DE ACCESO REQUISITOS DE ACCESO PROCESO DE GESTIÓN DE DERECH. ACCESO LOCAL (LOCAL LOGON) ACCESO REMOTO (REMOTE LOGIN)	[OP.ACC] [OP.ACC.2] [OP.ACC.4] [OP.ACC.6] [OP.ACC.7]
Gestión de activos	(GA)	A.8 Gestión de activos	ADQUISICIÓN DE NUEVOS COMPONENTES INVENTARIO DE ACTIVOS GESTIÓN DE CAMBIOS	[OP.PL.3] [OP.EXP.1] [OP.EXP.5]
Auditoría y trazabilidad	(AT)	9 Evaluación del desempeño 9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 9.3 Revisión por la dirección A.12.4 Registros y supervisión	REGISTRO DE LA ACTIVIDAD DE USUARIOS PROTECCIÓN DE REGISTROS DE ACTIVIDAD	[OP.EXP.8] [OP.EXP.10]
Formación y Concienciación	(FC)	7.3 Concienciación	FORMACIÓN	[MP.PER.4]
Gestión de configuraciones	(GC)	A.8.1.1 Inventario de activos A.8.1.4 Devolución de activos	ARQUITECTURA DE SEGURIDAD ADQUISICIÓN DE NUEVOS COMPONENTES DIMENSIONAMIENTO/GESTIÓN CAPACIDAD INVENTARIO DE ACTIVOS CONFIGURACIÓN DE SEGURIDAD GESTIÓN DE LA CONFIGURACIÓN	[OP.PL.2] [OP.PL.3] [OP.PL.4] [OP.EXP.1] [OP.EXP.2] [OP.EXP.3]
Identificación y autenticación	(IA)	A.9 Control de acceso A.9.2 Gestión de acceso de usuario A.9.4 Control de acceso a sistemas y aplicaciones A.10 Criptografía	IDENTIFICACIÓN MECANISMO DE AUTENTICACIÓN	[OP.ACC.1] [OP.ACC.5]
Respuesta a incidentes	(RI)	A.16 Gestión de incidentes de segur. información	GESTIÓN DE INCIDENCIAS	[OP.EXP.7]
Mantenimiento	(MA)	10 Mejora 10.1 No conformidad y acciones correctivas 10.2 Mejora continua A.14 Adquisición, desarrollo y mantenim. de SSII	MANTENIMIENTO	[OP.EXP.4]

En la tabla de la izquierda 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.

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.

Protección de medios	(PM)	A.8.3 Manipulación de los soportes A.8.3.1 Gestión de soportes extraíbles A.8.3.2 Eliminación de soportes A.8.3.3 Soportes físicos en tránsito	MEDIOS ALTERNATIVOS REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO	[OP.EXT.9] [MP.IF.7]
Seguridad personal	(SP)	A.7 Seguridad relativa a los recursos humanos	GESTIÓN DEL PERSONAL	[MP.PER]
Seguridad física	(SF)	A.11 Seguridad física y del entorno	MEDIDAS DE PROTECCIÓN	[MP]
Recuperación	(RE)	A.12.3 Copias de seguridad A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio 17.2 Redundancias. 17.2.1 Disponibilidad recursos tratam. información	CONTINUIDAD DEL SERVICIO	[OP.CONT]
aGestión de riesgos	(GR)	6.1 Acciones para tratar los riesgos y oportunidades 6.1.2 Apreciación de riesgos de seguridad información 6.1.3 Tratamiento de riesgos de segur. información 8.2 Apreciación de los riesgos de seguir. información 8.3 Tratamiento de riesgos de seguridad información	ANÁLISIS DE RIESGOS ANÁLISIS DE IMPACTO	[OP.PL.1] [OP.CONT.1]
Evaluaciones de seguridad	(ES)	9 Evaluación del desempeño 9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 9.3 Revisión por la dirección A.5.1.2 Revisión de políticas para la segur.información A.12.7 Consideraciones sobre la auditoria de SSII A.12.7.1 Controles de auditoría de SSII A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	PRUEBAS PERIÓDICAS	[OP.CONT.3]
Conciencia situacional (Ciberinteligencia)	(CS)	A.6.1.3 Contacto con las autoridades A.6.1.4 Contacto con grupos de interés especial A.6.1.5 Segur. información en la gestión de proyectos A.12.1 Procedimientos y responsabil. operacionales A.18 Cumplimiento	MONITORIZACIÓN DEL SISTEMA	[OP.MON]
Protección de sistemas y comunicaciones	SC)	A.12 Seguridad de las operaciones A.13 Seguridad de las comunicaciones A.14 Adquisición, desarrollo y mantenimiento de SSII A.15 Relación con proveedores A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	MEDIDAS DE PROTECCIÓN PROTECCIÓN DE LOS EQUIPOS PROTECCIÓN DE LAS COMUNICACIONES PROTECCIÓN DE LOS SERVICIOS	[MP] [MP.EQ] [MP.COM] [MP.S]

En este documento analizaremos un Plan Director de Seguridad (**PDS**) sobre la base de normativas y referentes de la industria, poniendo especial hincapié en un método práctico y eficiente para confeccionarlo.

En el año 2018, publiqué un artículo llamado:

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

En el mismo relacionaba los pasos a seguir sobre la base de una publicación de **INCIBE**.

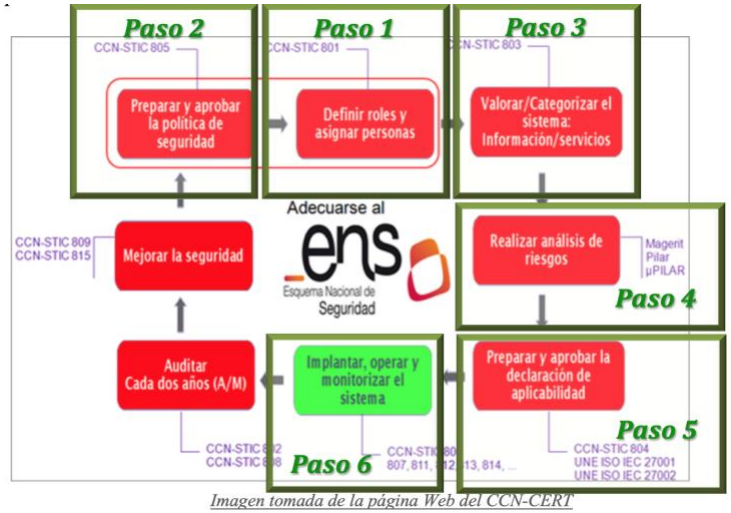


Imagen tomada de la página Web del CCN-CERT

El **ENS** es que define tres categorías: **BÁSICA**, **MEDIA** o **ALTA** ⇨ las que dependen directamente del Impacto: **Limitado**, **Grave** o **Muy grave**.
Por lo que evidentemente nos veremos obligados a estudiar ¿cómo es esto del Impacto?

Dimensiones ⇨ Impacto ⇨ Nivel ⇨ Categoría

Integridad de la información y de los sistemas	(IS)	7 Soporte A.12.1.4 Separación de los recursos de desarrollo, prueba y operación A.12.2 Protección contra el SW malicioso (malware) A.12.2.1 Controles contra el código malicioso A.14.2.1 Política de desarrollo seguro A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo A.14.2.4 Restricciones a cambios en paquetes de SW A.14.2.5 Principios de ingeniería de sistemas seguros A.14.2.6 Entorno de desarrollo seguro	PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS (SW) PROTECCIÓN DE LA INFORMACIÓN	[MP.SI] [MP.SW] [MP.INFO]
NO considera		Cuerpo de la Orden 4. Contexto de la organización 5 Liderazgo 6 Planificación A.5 Políticas de seguridad de la información A.6 Organización de la seguridad de la información	MARCO ORGANIZATIVO	[ORG]
NO considera		A.15 Relación con proveedores	SERVICIOS EXTERNOS	[OP.EXT]
NO considera		A.18 Cumplimiento	NO considera	

Tomemos también como referencia para seguir avanzando, las fases que propone otra publicación, también de **INCIBE** llamada: "**Plan Director de Seguridad**"

(Podéis descargarla AQUÍ)

Ilustración 1
Implantando un Plan Director de Seguridad

En este documento analizaremos un Plan Director de Seguridad (**PDS**) sobre la base de normativas y referentes de la industria, poniendo especial hincapié en un método práctico y eficiente para confeccionarlo. Para que esto sea eficiente, **la Dirección debe estar involucrada de lleno**.

Como podemos ver en el flujo de INCIBE, todo comienza por **conocer la situación actual.**

Reitero el concepto que vengo afirmando desde hace meses:

"Lo crítico es la INFORMACIÓN… no las infraestructuras"

Propongo que no planifiquemos sobre la "caja fuerte" sino en lo que está dentro. Esta será la línea de pensamiento a seguir en este PDS.

La clave para saber por donde empezar es el "Impacto" (*como se mencionó en el ENS*) para poder determinar qué es **crítico** y que no lo es.

A partir del capítulo 6 del libro "**Manual de la Resiliencia**" está explicado todo el detalle de esta actividad (podéis descargarlo AQUÍ)

Hasta ahora:

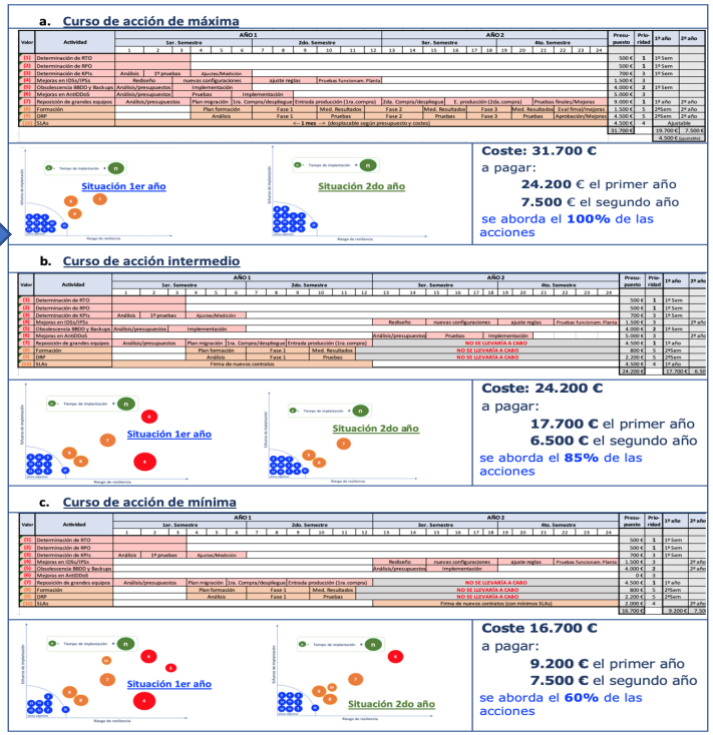
- Hemos comparado tres referencias importantes (**CMMC-ISO27002-ENS**)
- Identificamos una situación inicial, con su riesgo e impacto (Fase 1 flujo **INCIBE**)
- Calculamos el riesgo e impacto de la "información crítica" (libro "Manual de la Resiliencia")

¡Sigamos avanzando entonces!

Seleccionemos ahora los "Controles o dimensiones" (*o como los queráis llamar*) de la tabla comparativa de (**CMMC-ISO27002-ENS**) centrándonos inicialmente en lo relacionado con "**Muy grave** o **Alta**"

Al abordar el tema de un PDS, muchos sitios recomiendan definir un "alcance". En mi humilde opinión esto debería considerarse únicamente para una gran organizazión (pero muy ,muy grande). Para cualquier otra empresa, es necesario proteger toda la información crítica, no solo parte ella, por lo que me decanto por planificar bien el avance del "ciclo de vida de la seguridad" cubriendo el 100% de lo evaluado, pero a través de una planificación progresiva y al menos "**bi anual**" con rigurosos **hitos de control**.

Volvamos al libro "**Manual de la Resiliencia**"
En el capítulo 9. "Estrategias Resilientes en Redes y Sistemas"
Se presenta un plan bi anual con tres cursos de acción diferentes, para que la Dirección pueda decidir por uno de ellos.



El toque final lo daría considerando los niveles de madurez que propone **CMMC**, y para seros absolutamente sinceros, los primeros años los "***españolizaría***" bastante (*esto me va costar muchas críticas…*)

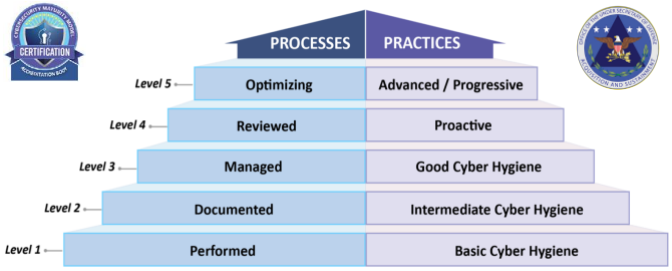
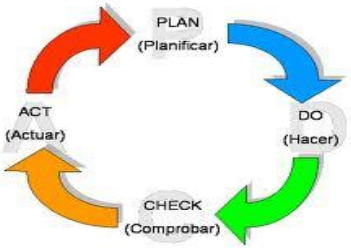


Figure 2. CMMC Levels and Descriptions

Luego implantando un adecuado ciclo "**PDCA**" podemos mantenerlo en rumbo, por medio de "métricas" (*por ej. Las que propone **ISO-27004,** verlas también en el libro mencionado*).



CMMC propone:

Nivel	Procesos	Prácticas
nivel 1	Ejecutado	Higiene básica de Ciber
nivel 2	Documentado	Higiene intermedia de Ciber
nivel 3	Gestionado	Buena higiene de Ciber
nivel 4	Revisado	Proactivo
nivel 5	Optimizado	Avanzado / Progresivo

Al "españolizarlo", me refiero a la parte final que debemos tener en cuenta, es decir ser "prácticos", lo que intento decir es que:

- **N1 – Ejecutado:** Solo funciona y nada más.
- **N2 – Documentado:** Existe un procedimiento escrito (y tal vez inicialmente implantado).
- **N3 – Gestionado:** Procedimentado y eficazmente implantado.
- **N4 – Revisado:** Ha pasado por revisiones, auditorías y entra en un segundo ciclo de vida.
- **N5 – Optimizado:** Ya se han comenzado a implantar acciones de mejora en 2º o más ciclos.

Los responsables de este PDS deberían ser capaces de "agendar" hitos de control, por ejemplo semestralmente basados en las métricas, como lo indica **ISO-27004** y "supervisar" su grado de avance, por ejemplo en los niveles de madurez que propone **CMMC**, y mi consejo "práctico" es que lo hagamos un poco "españolizado", es decir considerando lo que se acaba de indicar en el cuadro superior derecho, e ir evaluando si cada una de la acciones planificadas, se encuentra Ejecutada, Documentada, Gestionada, etc. sencillamente considerando lo que acabo de españolizar.

El objetivo final de un PDS debería ser "**llegar al nivel 5 de CMMC**", pero por supuesto no puede (ni debe) ser de un saque, sino de forma planificada y metódica. Nuestro primer PDS bianual, debería sentar las bases de este camino hasta lograr el objetivo final (en el tiempo que la empresa necesite).

Resumen final:

- Hemos comparado 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 Reiliencia 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.

www.darFE.es

¡Nos vemos dentro de dos años!