# **Seguridad en la capa de enlace de datos y capa de red con sus nuevos paradigmas**

## RELACIONES EXISTENTES ENTRE NORMATIVAS Y LOS ECOSISTEMAS DE TI

Normas ISO 27000: Familia de estándares de ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporciona un marco para la gestión de la seguridad

* Conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI
* Normas base: 20001, 20002
* Normas complementarias: 20003, 20004, 20005, ...

Seguridad de la información (según ISO 27001): preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas implicados en su tratamiento

* Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
* Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
* Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

ISO/IEC 27000: define el vocabulario estándar empleado en la familia 27000 (definición de términos y conceptos)

ISO/IEC 27001: especifica los requisitos a cumplir para implantar un SGSI certificable conforme a las normas 27000

* Define cómo es el SGSI, cómo se gestiona y cúales son las resposabilidades de los participantes.
* Sigue un modelo PDCA (Plan-Do-Check-Act)
* Puntos clave: Gestión de riesgos + Mejora contínua

# CMM/CMMI

El modelo CMM define que deben existir algunas áreas o procesos clave en la organización que deberán realizar alguna función específica. A estas áreas se les denomina como Áreas Clave de Proceso (KPA - Key Process Area).

El modelo define para cada una de estas áreas un conjunto de buenas prácticas, dependiendo de que tanto se ajusten estas áreas con el modelo CMM se puede conocer el nivel de madurez de esta organización.

El modelo CMM y el modelo CMMI - Capability Maturity Model Integration se diferencian básicamente en que el primero se enfoca principalmente a las organizaciones o áreas de Tecnologías de información en cambio el modelo CMMI como su nombre lo indica es un modelo integrado y mejorado que se puede aplicar a un número mayor de organizaciones de diferentes sectores.

El modelo CMM define 5 niveles de madurez:

1 - Inicial. Es el primer nivel es decir que no es necesario hacer ningún esfuerzo para llegar aquí, las organizaciones en este nivel no disponen de un ambiente adecuado para el desarrollo de software. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. Los procesos varían según los individuos, el éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobre costos. El resultado de los proyectos es impredecible y esta pobremente controlado.

2 - Repetible. En este segundo nivel se encuentran las empresas en las que existe planificación y seguimiento de proyectos y está implementada la gestión de los mismos. No obstante, aún existe un riesgo significativo de no cumplir las metas.

3 - Definido. Existe un conjunto establecido de procesos estándar globales bien definidos (estableciendo sus objetivos) dentro de la organización. Existe un sistema de gestión de los proyectos. Una diferencia crítica entre los niveles 2 y 3 de madurez es el alcance de los estándares, descripciones de los procesos y procedimientos. En el nivel 2 pueden variar entre las distintas instancias de los procesos (entre diferentes proyectos); a nivel 3 son globales dentro de la organización e igual en todas las instancias de cada proceso.

4 - Gestionado. Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad.

5 - Optimizado. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

# EFQM

El Modelo Europeo de Excelencia Empresarial, conocido como Modelo EFQM está patrocinado por la EFQM y la Comisión de la UE, base del Premio Europeo a la Calidad.

El Modelo EFQM es un modelo no normativo, cuyo concepto fundamental es la autoevaluación basada en un análisis detallado del funcionamiento del sistema de gestión de la organización usando como guía los criterios del modelo.

Esto no supone una contraposición a otros enfoques (aplicación de determinadas técnicas de gestión, normativa ISO, normas industriales específicas, etc.), sino más bien la integración de los mismos en un esquema más amplio y completo de gestión.

La utilización sistemática y periódica del Modelo EFQM por parte del equipo directivo permite a éste el establecimiento de planes de mejora basados en hechos objetivos y la consecución de una visión común sobre las metas a alcanzar y las herramientas a utilizar. Es decir, su aplicación se basa en:

* La comprensión profunda del modelo por parte de todos los niveles de dirección de la empresa.
* La evaluación de la situación de la misma en cada una de las áreas.

El Modelo EFQM consta de dos partes:

* Un conjunto de criterios de excelencia empresarial que abarcan todas las áreas del funcionamiento de la organización.
* Un conjunto de reglas para evaluar el comportamiento de la organización en cada criterio. Hay dos grupos de criterios:
* Los Resultados (Criterios 6 al 9) representan lo que la organización consigue para cada uno de sus actores (Clientes, Empleados, Sociedad e Inversores).
* Los Agentes (Criterios 1 al 5) son aspectos del sistema de gestión de la organización. Son las causas de los resultados. Para cada grupo de criterios hay un conjunto de reglas de evaluación basadas en la llamada “lógica REDER”.