



# Calidad y seguridad en los sistemas de información

## La importancia de un enfoque global

«LA SEGURIDAD DEBE SER UNA DE LAS CARACTERÍSTICAS INCLUIDAS DENTRO DE LA CALIDAD. SI UN SISTEMA NO ES SEGURO, NO ES FIABLE POR TANTO NO PUEDE SER DE CALIDAD»



**Senén J. Pájaro Novoa**

**PRESIDENTE DE  
AFSMI,  
DIRECTOR DE  
CALIDAD FUJITSU  
ESPAÑA**

**L**os Sistemas de Información y Comunicaciones son un pilar esencial para el éxito de cualquier organización. Sin disponer de información eficaz, fiable, fácilmente accesible desde donde se necesite y cuando se necesite, no es posible prestar la adecuada atención a los clientes, cumplir con los compromisos adquiridos, optimizar y mejorar los procesos, aumentar la productividad y capacidad competitiva. La información, debidamente gestionada, almacenada y distribuida es el motor que propulsa la permanente adaptación de una organización a su entorno, condicionando no solo su éxito sino su supervivencia en un marco cada vez más cambiante y dominado por las

características que impone la globalización.

Los Sistemas de Información deben reunir las condiciones de Calidad y Seguridad imprescindibles para el buen funcionamiento de la organización a la que prestan sus servicios. Podríamos utilizar muchas definiciones de Calidad para aplicarlas a un Siste-

**Una auditoría es un proceso mediante el cual se comprueba que el sistema funciona según las normas de seguridad establecidas**

ma de Información pero creo que la más sencilla de todas es la que mejor se adapta: Un Sistema de Información es «de Calidad» si cumple los requerimientos o requisitos para los que ha sido diseñado, implantado, mantenido

y actualizado. La Seguridad debe ser una de las características incluidas dentro de la Calidad. Si un Sistema no es seguro, no es fiable por tanto no puede ser de Calidad. La seguridad depende de muchos factores: la arquitectura del hardware y software, del propio hardware y software, la conexión con otras redes y los accesos





externos desde clientes, proveedores y el personal propio, las normas y procedimientos de utilización del sistema, la aptitud y actitud de los responsables y administradores del sistema, la actitud y aptitud de los usuarios internos, la estructura física de los edificios y oficinas donde esté instalado el sistema, etc. La complejidad de los factores es

tal que si no contemplamos la organización como un todo, en una visión holística e integrada, seguramente lograremos tener aspectos seguros en nuestros sistemas, pero no seguridad real. La seguridad hay que promoverla activamente desde Dirección, hay que gestionarla de forma permanente, hay que verificarla periódicamente. Una

forma de verificarla es mediante las Auditorías que son parte de los procesos de gestión. Una auditoría es un proceso mediante el cual se comprueba, mediante el análisis de evidencias documentales, que el sistema funciona según las normas de seguridad establecidas. Esto implica que haya normas de seguridad claras y evidencias



## MODELO EXCELENCIA EFQM



documentales que demuestren que aquellas se siguen estrictamente. Debe existir en la organización una cultura de calidad y seguridad adecuadas, esto solo puede lograrse de forma efectiva, si existe un MODELO DE GESTION que propugne estos y otros valores. Un ejemplo es el MODELO DE EXCELENCIA de la EFQM, cuyos criterios se exponen en la Fig. 1:

### Modelo de excelencia de la EFQM

La idea básica que fundamenta el Modelo EFQM es la conocida como ciclo de Deming, que consiste en:

- **Planifica lo que se debe realizar,**
- **Ejecuta lo planificado,**
- **Verifica los resultados que obtienes ; y**
- **Actúa corrigiendo las desviaciones.»**

El Modelo consta de 9 criterios: Cinco que son los AGENTES, las causas que producen los cuatro criterios de RESULTADOS. En el conjunto de los cuatro tipos de Resultados podemos identificar los grupos de interés en la organización, que están afectados:

■ **Los Accionistas** que tendrán un alto nivel de satisfacción si se logran buenos resultados de negocio/performances.

■ **El personal de la organización** que estará satisfecho si se producen resultados que le impacten positivamente.

■ **La sociedad en general**, estará satisfecha con la organización si ésta le aporta valor a través de las formas más diversas.

Debemos analizar los resultados logrados, medirlos, aprender de ellos y utilizar el aprendizaje para actuar sobre los agentes o causas e implantar acciones de mejora que nos permitan alcanzar nuevas metas. Este es un bucle que nos debe llevar hacia la mejora continua, entendida como la continua mejor adaptación a las circunstancias cambiantes en las que debe desarrollar su actividad la organización.

Ninguna organización sobrevive largo tiempo sin una adecuada **Política y Estrategia** y aquí están incluidos la visión y misión, los valores y principios, los objetivos estratégicos y las estrategias para lograrlos. Es la Dirección la que tiene la responsabilidad de estos conceptos y para llevarlos a efecto de forma eficaz, debe de tener definidos, gestionados y controlados los procesos necesarios.

**El Liderazgo** es el proceso mediante el cual la Dirección ejerce su responsabilidad, cómo comunica con el

*El Liderazgo es el proceso mediante el cual la Dirección ejerce su responsabilidad, en definitiva cómo hace que todos participen en el logro de los objetivos de la organización*

■ **Los Clientes**, el activo más importante de cualquier organización, que estarán satisfechos si la organización cumple sus compromisos, es fiable, flexible, competitiva.



personal, cómo escucha, en definitiva cómo hace que todos participen en el logro de los objetivos de la organización. La Dirección, ejerciendo su liderazgo, debe poner en marcha acciones que faciliten que cada miembro de la organización, cualquiera que sea su posición en el organigrama, ponga el máximo de su capacidad y esfuerzo en el logro de los objetivos que se propongan.

**La Gestión del Personal**, cómo se selecciona, cómo se forma y entrena, cómo se le reconoce y promueve. El personal es el recurso más valioso de cualquier organización. Son quienes atienden a los clientes, quienes desarrollan los productos y servicios, quienes en definitiva pueden realizar un esfuerzo extra para satisfacer cualquier demanda puntual. La experiencia nos dicta que primero está el cliente y luego el personal, dentro del natural orden de prioridades.

**La Gestión de otros Recursos** es también fundamental para lograr el éxito de cualquier organización, en este criterio el Modelo de Excelencia incluye edificios, maquinaria, activos financieros, sistemas de información,

gestión del conocimiento, acuerdos con subcontratistas y proveedores.

El elemento central del Modelo de Excelencia son los **PROCESOS**. Todo en una organización se logra a través de los procesos.

### Procesos

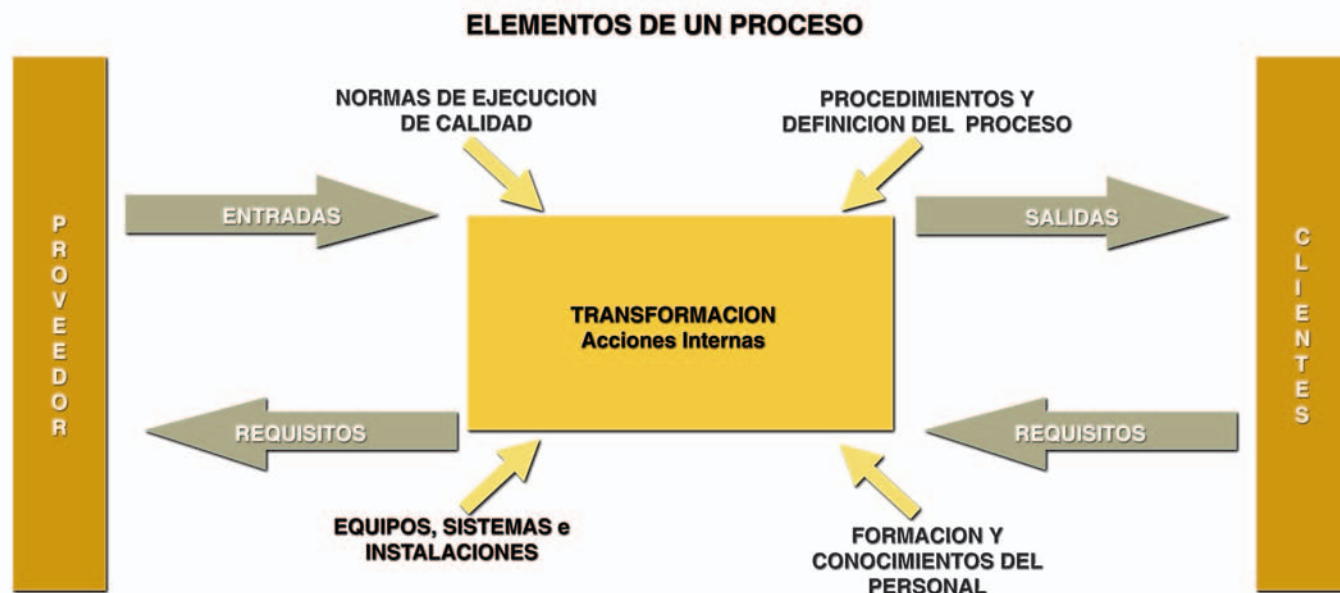
Un Proceso es una acción o secuencia de acciones realizadas para lograr un resultado, salida o output transfor-

mental de cualquier proceso es satisfacer los requerimientos del cliente. Por tanto ante cualquier proceso debemos identificar quien es el cliente, que demanda del proceso es decir cuales son sus requerimientos, como, donde y cuando debemos entregar los resultados. Conocidos los resultados y sus requerimientos, atributos o características tenemos que identificar los requerimientos de las entradas del proceso y transmitirlos al proveedor. Es realmente una cadena cuya acción va desde las entradas a los resultados pero para que funcione adecuadamente es imprescindible identificar los requerimientos desde los resultados hasta las entradas.

Los procesos de una organización no solo forman cadenas de valor sino redes. Unos interactúan con otros, constituyen un sistema que debe ser analizado en su conjunto para lograr los objetivos planteados. Hay procesos estratégicos y de dirección, procesos de soporte como la selección y formación del personal, la gestión de las TIC, etc.; y procesos operativos o de negocio que son aquellos en los cuales se realizan las acciones que crean valor para los

Debe existir en la  
organización una cultura  
de calidad y seguridad  
adecuadas

mando o combinando unas entradas o inputs. Las salidas de un proceso suelen ser las entradas de otro proceso al que llamamos cliente. Las entradas de un proceso son las salidas de otro al que llamamos proveedor. Lo funda-







clientes. En la Fig. 2 pueden verse los elementos de un proceso.

Cada proceso debe tener un responsable cuya principal misión es, no solo conocer y gestionar todos los elementos del mismo, si no tener identificadas medidas e indicadores que le permitan valorar las prestaciones de dicho proceso y su grado de cumplimiento con los requisitos del cliente, así como la evolución en el tiempo. Es necesario medir para aprender y consecuentemente poder mejorar. Existen múltiples herramientas de calidad para ser utilizadas en la mejora de procesos, cada una tiene su campo de apli-

## La calidad y la seguridad en el entorno de las TIC no pueden ser consideradas elementos aislados del resto de la organización

cación específico. Es bueno que el responsable del proceso conozca las herramientas más importantes; pero es mejor todavía que esté comprometido con la mejora continua, ya que si detecta que dicha mejora no se produce siempre podrá recurrir a expertos de calidad que le ayuden a identificar las causas, mediante el uso de las herramientas pertinentes.

El establecimiento de una cultura de mejora por parte de todos en la organización, en todo lo que hacen, es la mejor forma de afrontar los retos que se le presentan dentro de un entorno siempre cambiante.

En el entorno de las Tecnologías de la Información y las Comunicaciones existen procesos establecidos y que están basados en las mejores prácti-

cas. Un ejemplo en el entorno de los Servicios TIC es ITIL (IT Information Library) que recoge una serie de procesos como, gestión de la configuración, gestión de incidencias, gestión de problemas, etc. que gestionados de la forma que propone existe una posibilidad de éxito mucho más elevada ya que la librería está basada en las mejores prácticas. ITIL fue creada y es gestionada por una organización independiente y no lucrativa que es IT SMF (IT Service Management Forum). ITIL se convertirá próximamente en un estándar ISO (ISO 20000). En internet puede obtenerse más información en [www.itsmf.com](http://www.itsmf.com)

En el entorno de los proyectos de desarrollo de software existe otro modelo en creciente expansión y es CMMI (Capability Maturity Model Integration). Es un modelo que recoge cinco niveles de madurez de los procesos relacionados con el desarrollo de software, el nivel más bajo en el que podemos considerar los procesos organizados de forma caótica y por tanto con resultados imprevisibles; el nivel más alto el cinco donde todos los procesos están perfectamente organizados, medidos y gestionados. Que una organización pase de un nivel de madurez al siguiente supone esfuerzos que se cuantifican entre 9 y dieciocho meses. Evidentemente cuanto mayor sea el nivel de madurez de los procesos más fiables y previsibles serán los resultados. En internet [www.sei.com](http://www.sei.com) puede encontrarse más información sobre CMMI.

La expansión que está teniendo el uso de CMMI se debe sin duda al hecho de que un gran porcentaje de proyectos de desarrollo de software siguen sin finalizarse en tiempo, con costes superiores a los previamente estimados, sin cumplir todos los requerimientos pedidos. Esto ha sido así durante los últimos 50 años, bienvenida sea una herramienta que nos permita mejorar los resultados. ♦

## Calidad y seguridad

La calidad y la seguridad en el entorno de las TIC no pueden ser consideradas elementos aislados del resto de la organización. El disponer de un modelo de gestión que propugne la búsqueda de la excelencia a través de la mejora continua, y cuando sea posible de mejoras en escalón, en todos los procesos de la organización, es un condicionante fundamental. Ese modelo permitirá crear una cultura en la que todos aporten valor, todos se esfuercen en maximizar la eficacia y la eficiencia de sus procesos para proporcionar productos y servicios a los clientes. Todos asumirán como propias las medidas de seguridad de sus sistemas TIC para evitar que los potenciales problemas puedan impactar negativamente a sus clientes. Todos entenderán su red de procesos, comprenderán la importancia de gestionarlos y mejorarlos, aportarán sugerencias e ideas de mejora; en definitiva vivirán su actividad organizativa como una experiencia vital y enriquecedora. Las auditorías de Calidad o de Seguridad seguirán siendo necesarias como procesos objetivos que a través de evidencias documentales permitirán, no solo comprobar el cumplimiento de las normas establecidas, sino identificar puntos débiles y aspectos a mejorar que por medio de las acciones que correspondan también contribuirán al proceso de mejora de la organización. Nada permanece estable, todo cambia, en las organizaciones también, para mejor o para peor. La opción es obvia pero elegirla es cuestión de voluntad, inteligencia y saber hacer.