GENERALIDADES DE LA SEGURIDAD INFORMÁTICA 2

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

En la actualidad, las organizaciones se encuentran inmersas en un entorno competitivo y con cambios constantes cada vez más frecuentes. Es por ello que la calidad y mejora de procesos se convierten en un imperativo para la supervivencia de estas empresas, con el propósito de ofrecer productos y servicios a bajo coste, y que satisfagan los requerimientos de los clientes.

Las empresas necesitan gestionar sus actividades y recursos con la finalidad de orientarlos hacia la consecución de buenos resultados, mediante la adaptación de herramientas y metodologías que permitan a las organizaciones configurar su **Proceso de Gestión y Mejora Continua.**

Tabla de contenido

El método PDCA o rueda de Deming

La misma es la sistemática más usada para implantar un sistema de mejora continua cuyo principal objetivo es la autoevaluación, destacando los puntos fuertes que hay que tratar de mantener y las áreas de mejora en las que se deberá actuar.

Ciclo PDCA de mejora continua.

Éste ciclo de mejora continua está compuesto por cuatro etapas que son cíclicas, las cuales deben ser revaluadas periódicamente para incorporarle nuevas mejoras, a continuación abordaremos dichas etapas:

1- PLAN (planificar):
En esta fase se trabaja en la identificación del problema o actividades susceptibles de mejora, se establecen los objetivos a alcanzar, se fijan los indicadores de control y se definen los métodos o herramientas para conseguir los objetivos establecidos.
Una forma de identificar estas mejoras puede ser realizando grupos de trabajo o bien buscar nuevas tecnologías o herramientas que puedan aplicarse a los procesos actuales. Para detectar tecnologías o herramientas a veces es conveniente fijarse en otros sectores, esto aporta una visión diferente pero muchas de las soluciones pueden aplicarse a más de un sector.
2 – DO (hacer/ejecutar):
Llega el momento de llevar a cabo el plan de acción, mediante la correcta realización de las tareas planificadas, la aplicación controlada del plan y la verificación y obtención del feedback necesario para el posterior análisis.
En numerosas ocasiones conviene realizar una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala. La selección del piloto debe realizarse teniendo en cuenta que sea suficientemente representativo pero sin que suponga un riesgo excesivo para la organización.
3 – CHECK (comprobar/verificar):
Una vez implantada la mejora se comprueban los logros obtenidos en relación a las metas u objetivos que se marcaron en la primera fase del ciclo mediante herramientas de control (Diagrama de Pareto, listas de chequeo, indicadores, etc.)
Para evitar subjetividades, es conveniente definir previamente cuáles van a ser las herramientas de control y los criterios para decidir si la prueba ha funcionado o no.
4 – ACT (actuar):
Por último, tras comparar el resultado obtenido con el objetivo marcado inicialmente, es el momento de realizar acciones correctivas y preventivas que permitan mejorar los puntos o áreas de mejora, así como

extender y aprovechar los aprendizajes y experiencias adquiridas a otros casos, y estandarizar y consolidar metodologías efectivas.
En el caso de que se haya realizado una prueba piloto, si los resultados son satisfactorios, se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados sin desecharla.
Una vez finalizado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.
Algunos de los **beneficios** que proporcionan una adecuada mejora de procesos son los siguientes:

- TIMMING: se disminuyen tiempos, aumentando la productividad.
- QUALITY: se disminuyen errores, ayudando a prevenirlos.
- COST: se disminuyen recursos (materiales, personas, dinero, mano de obra, etc.), aumentando la eficiencia.

La norma ISO 20000

Esta es una norma del Sistema de Gestión de servicios. Especifica los requisitos que debe cumplir el proveedor de servicios para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGS. Los requisitos incluyen el diseño, la transición, la entrega y la mejora de los servicios para cumplir con los requerimientos del servicio.

Esta norma se presenta como el estándar internacional (ISO) para la gestión de servicios TI y que ha sido aceptado como un referente en este campo por la mayoría de los países del mundo. El objetivo de ISO 20000 es doble:

- Ayudar a las empresas a conseguir servicios de TI más efectivos
- Incorporar las mejores prácticas internacionales en la Gestión de Servicios TI (ITSM)

Cuando nos referimos a servicios TI nos estamos refiriendo a servicios cuya provisión depende de las tecnologías de la información y que pueden ser tanto Servicios a Clientes externos o servicios brindados a partes internas de la organización y necesarios para el desarrollo de la actividad de su negocio
En el objetivo de mejorar la gestión de servicios TI ISO 20000 nos proporciona

- Un conjunto de procesos de administración de servicios TI
- Un conjunto de buenas prácticas internacionales

Las normas ISO 270xx

Esta es la familia de normas de la Organización Internacional de Estandarización (ISO). Cada norma tiene reservado un número dentro de una serie que van desde 27000 hasta 27019 y desde 27030 hasta 27044.

Dentro de ésta serie tenemos las destacadas:

- ISO 27001: Sistemas de gestión de Seguridad de la información: establece unas condiciones de adaptación para aquellas empresas que se encuentren certificadas.
- ISO 27002: Es el manual de buenas practices en la que se describen los objetivos de control y evaluaciones recomendables en cuanto a la segurdidad de la información.

- ISO 27003: Es un amnual para implementar un Sistema de gestión de Seguridad de la información.
- ISO 27004: Aquí se especifican la técnicas de medida y las métricas que son aplicables a la determinación de la eficacia de un Sistema de gestión de Seguridad de la información.
- ISO 27005: Esta norma establece las diferentes directrices para la gestión de los riesgos en la Seguridad de la información.
- ISO 27006: Aquí se especifican todos los requisitos para lograr la acreditación de la sentridades de auditoria y certificación de Sistemas de gestión de Seguridad informatica.
- ISO 27007: Manual de auditoria de un Sistema de gestión de Seguridad de la información.
- ISO 27011: Guía de la gestión de la Seguridad de la información específica para telacomunicaciones.
- ISO 27031: Guía de continuidad del Negocio basada en las tecnologías de la información y las comunicaciones (TIC).
- ISO 27032: Es un estándar que garantiza las directrices de Seguridad que desde la ISO han asegurado que proporcionará una colaboración general entre las multiples partes interesadas para reducier riesgos en INTERNET.
- ISO 27033: Norma derivada de la norma de Seguridad ISO/IEC 18028 de la red, y dá una vision general de Seguridad de la red y de los conceptos asociados.
- ISO 27034: Es una guía de Seguridad en aplicaciones.

Conclusiones y reocmendaciones

En conclusión, un sistema de gestión de la calidad permite a una organización desarrollar políticas, establecer objetivos y procesos, y tomar las acciones necesarias para mejorar su rendimiento. En este contexto resulta de gran utilidad utilizar la metodología PDCA impulsada por Deming, como una forma de ver las cosas que puede ayudar a la empresa a descubrirse a sí misma y orientar cambios que la vuelvan más eficiente y competitiva.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica