2.1 Cumplimiento ISO 27001

El SGSI de la ISO 27001 es bastante amplio y muchas empresas no son conscientes de las carencias o necesidades que tienen relativas a seguridad de la información hasta que deciden implantarlo. Apoyándonos del formulario online en esta dirección:

https://advisera.com/27001academy/es/herramienta-gratuita-analisis-de-brecha-para-iso-27001/

Se pide completar y responder todas las preguntas de las secciones 4 a la 10 (recomendamos registrar un correo electrónico para guardar el formulario mientras lo completáis) y comprobar la modificación que sufre el valor indicado en REQUISITOS DE PREPARACIÓN. Este valor trata de mostrar de forma simbólica y representativa una aproximación al estado actual de integración del SGSI en la empresa, mostrando la "importancia" de cumplir con los requisitos, sin tener consideraciones respecto a los controles implementados (Anexos).

Teniendo en cuenta dicho valor de REQUISITOS DE PREPARACIÓN, comentad aquellas preguntas del formulario que más os llamen la atención por el peso total que adquieren dentro de su sección y en el total. Y si creéis que merecen un peso tan elevado/inferior según vuestro criterio.

Los bloques de operación y evaluación del desempeño son los que mas peso tienen, y tiene bastante sentido. Ya que no tiene mucha lógica que tengas un alto % de puntos en los requisitos de preparación de un SGSI cuando no haces las operaciones necesarias y no evalúas las mismas.

Es seguido por soporte, planificación y contexto de la organización, lo cual tampoco me sorprende. Ya que sin unos medios adecuados, una buena planificación correcta y sin conocer en que punto se encuentra tu organización, no es posible tener un buen SGSI.

Las dos últimas categorías son liderazgo y mejora, que estas si que me han sorprendido un poco. Ya que en una organización el liderazgo y como fluye por la misma lo considero muy importante. De que nos sirve tener un gran SGSI si mi manager no lo cumple… o lo cumple porque no lo que queda otra pero su opinión del mismo es que no sirve para nada¿? En estos casos tenemos un problema.

Como he comentado en el ejercicio 1 el tema de la mejora es muy importante en una organización y que este en último lugar y con bastante diferencia del primer contexto, no me parece adecuado. El ejemplo es parecido al caso anterior, ¿de qué nos sirve una gran SGSI a día de hoy del año 1978? Los espacios para proponer y realizar mejoras son muy importantes dentro de las organizaciones.

También me ha chocado que no hubiese nada referente a la formación. Porque podemos cumplir todo y ¿si una de las personas que trabaja en nuestra organización no sabe que debe abrir un fichero adjunto que le ha llegado en un email en un lenguaje raro? Las personas de la organización tienen que tener nociones, aunque sea básicas, sobre seguridad de la información.