Parte II: Herramientas de autoevaluación de la normativa ISO/IEC 27001,27002

Para esta parte de la sesión debéis considerar una empresa, que puede ser real (si conocéis alguna lo podéis hacer con ella) o ficticia, sobre la que se va a hacer un diagnóstico respecto al grado de cumplimiento de la norma ISO/IEC 27001, asumiendo que tiene ciertas medidas de seguridad (técnicas y organizativas) ya implantadas. Para ello se cubrirán dos cuestionarios, el primero para ver el grado de cumplimiento de la norma ISO/IEC 27001, y el segundo, sobre la guía de buenas prácticas (27002).

1.- Cuestionario ISO/IEC 27001 (SGSI). Norma certificable.

- Abrid el cuestionario de auditoría (archivo Excel). Leed las instrucciones para cumplimentar la hoja. Dentro de la primera pestaña (*Compliance Checklist*), indicad un porcentaje de cumplimiento para cada control (grado de madurez del control). Explicad qué representa la columna "*Findings*" y poned para alguno de los controles algún ejemplo de "*Finding*" que podría darse en una auditoría real. No es necesario cubrir este campo para todos los elementos, basta con cinco o seis.
- Revisad los resultados finales de cumplimiento de cada uno de los apartados, comentando cuál es el mejor y cuál el peor, y la posible razón.

*Adjuntad el archivo Excel a la práctica (**añadiendo vuestro nombre al nombre de fichero**).*

2.- Cuestionario ISO/IEC 27002. Buenas prácticas de seguridad.

- Abrid el cuestionario de autodiagnóstico (archivo Excel) y responded sobre cada uno de los controles de los distintos capítulos de la norma, poniendo para algunos (no es necesario para todos) de los elementos del cuestionario la razón de la puntuación asignada, y las posibles mejoras que recomendaríais.
- Igual que en el caso anterior, revisad el resultado global, comentando los resultados de cumplimiento de cada uno de los capítulos, indicando cuál es el mejor y el peor.

*Adjuntad el archivo Excel a la práctica (**añadiendo vuestro nombre al nombre de fichero**).*