Auditoría y Legislación Informática.

Escuela Politécnica de Cáceres.

Práctica 4. Auditoría de ciberseguridad holística empresarial

Sesión 4

Te estás preparando para ser auditor de ciberseguridad. Vas a practicar lo que una organización debería hacer para orquestar una buena ciberseguridad en torno a sus activos, de forma que seas capaz de identificar carencias y proponer acciones correctivas, cuando corresponda, a la organización que audites. Estas empresas seguirán un modelo holístico de ciberseguridad basado en el marco de trabajo de *CyberTOMP*.

En esta sesión trabajaremos el concepto de dimensiones o facetas de la ciberseguridad. Se trata de comprender las diversas dimensiones de la ciberseguridad, que agrupan actuaciones de ciberseguridad encaminadas a un fin superior común, y reconocer la imposibilidad de garantizar la ciberseguridad de un activo sin abordar cada una de estas dimensiones.

Ejercicio 1. Toma tres activos de negocio imaginarios al azar, uno catalogado con criticidad baja, otro con media y un tercero catalogado con alta.

a) ¿Cuántas funciones de ciberseguridad podrían potencialmente contribuir a la ciberseguridad para cada uno de los activos? Y para cada una de ellas ¿Cuántas categorías distintas? Ayúdate de FLECO Studio para averiguar esto, creando estos tres casos, vacíos, y contando los valores preguntados, que se encuentran en la primera columna de la aplicación. Anótalos. No es necesario guardar los casos.

b) ¿Qué relación observas entre el número distinto de funciones, categorías, actuaciones y el nivel de criticidad del activo? ¿Te parece razonable?

Ejercicio 2. A continuación, abre el caso *1_Sesion_4_IG1.fleco*. Se corresponde con un activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,29974717. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, deben seguir sin aplicarse. En este caso son las funciones de ciberseguridad *Identificar* (ID) y *Detectar* (DE), así como todas las categorías y actuaciones de ciberseguridad derivadas.
- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar. Es decir, que tengan una mayor contribución a la ciberseguridad del activo aprovechando que ya están aplicándose.
- El nivel global buscado, de ciberseguridad del activo, es de al menos 0,5.

a) Modifica manualmente los valores de la columna *Current status* para obtener una serie de valores que cumplan con los objetivos definidos en las columnas *Constraint operator* + *Constraints value*. Cuando lo tengas hecho, guárdalo como *1_Sesion_4_IG1_manual.fleco*.

b) A la vista de lo realizado en el ejercicio ¿has identificado alguna forma de mejorar la ciberseguridad de un activo? ¿Implicaría un esfuerzo para áreas que hasta ahora no estaban aportando a la ciberseguridad de dicho activo? ¿Y más trabajo para las que ya estaban aportando?

Ejercicio 3. A continuación, abre el caso 2_Sesion_4_IG1.fleco. Se corresponde con un activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, deben seguir sin aplicarse. En este caso son las funciones de ciberseguridad "Identificar" (ID) y "Detectar" (DE), así como todas las categorías y actuaciones de ciberseguridad derivadas.
- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar. Es decir, que tengan una mayor contribución a la ciberseguridad del activo aprovechando que ya están aplicándose.
- El nivel global buscado, de ciberseguridad del activo, es de al menos 0,6 (en lugar de 0,5 del ejercicio anterior).

a) Modifica manualmente los valores de la columna *Current status* para obtener una serie de valores que cumplan con los objetivos definidos en las columnas *Constraint operator* + *Constraints value*. Si no consigues superar o igualar el 0,6 de ciberseguridad global del activo, obtén el valor más cercano y para en ese momento. Cuando tengas hecha una u otra cosa, guárdalo como *2_Sesion_4_IG1_manual.fleco*.

b) A la vista de lo realizado en el ejercicio ¿has conseguido el objetivo global de ciberseguridad del activo? ¿Por qué crees que has obtenido el resultado que has obtenido? ¿Qué habría hecho falta para poder tener un resultado mejor?

Ejercicio 4. A continuación, abre el caso *3_Sesion_4_IG1.fleco*. Se corresponde con un activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, pueden comenzar a aplicarse.
- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar.

- El nivel global buscado, de ciberseguridad del activo, es de al menos 0,6.

a) Modifica manualmente los valores de la columna *Current status* para obtener una serie de valores que cumplan con los objetivos definidos en las columnas *Constraint operator* + *Constraints value*. Cuando lo tengas hecho, guárdalo como *3_Sesion_4_IG1_manual.fleco*.

b) A la vista de lo realizado en el ejercicio ¿has conseguido el objetivo global de ciberseguridad del activo? ¿Qué diferencia este caso del descrito en el ejercicio anterior? ¿Qué implicaciones tiene sobre las dimensiones aplicadas al activo? ¿Están más o menos equilibradas?

Ejercicio 5. A continuación, abre el caso 4_Sesion_4_IG1.fleco. Se corresponde con un activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene un único objetivo/restricción estratégica de ciberseguridad definida, consistente básicamente en:

- El nivel global de ciberseguridad del activo buscado es exactamente 1.0, es decir, el 100%.

a) Modifica manualmente los valores de la columna *Current status* para obtener una serie de valores que cumplan con los objetivos definidos en las columnas *Constraint operator* + *Constraints value*. Cuando lo tengas hecho, guárdalo como *4_Sesion_4_IG1_manual.fleco*.

b) A la vista de lo realizado en el ejercicio ¿Es posible conseguir un valor global de ciberseguridad del activo de 1,0 (100%)? ¿Qué tiene que ocurrir para que esto sea posible? ¿Hay más de una forma de conseguir este estado?

Al finalizar esta sesión deben quedar claras dos ideas:

1. El número de facetas/dimensiones de la ciberseguridad que potencialmente aplicarían a la ciberseguridad de un activo es proporcional a la criticidad del activo de negocio y el impacto provocado por un ciberataque al mismos. Esto es lo que justifica una mayor dedicación de recursos a cubrir cada uno de los aspectos posibles.
2. La forma de aplicar una ciberseguridad mayor es: que para las dimensiones que ya estén aplicándose al activo se implementen de una forma más intensa las actuaciones de ciberseguridad asociadas que ya se hubieran implementado parcialmente o que se implementen actuaciones de ciberseguridad asociadas, que no se hubieran comenzado a implementar aún. Lo primero tiene un alcance limitado mientras que lo último permite lograr incluso un nivel del 100% de ciberseguridad global del activo.