Auditoría y Legislación Informática.

Escuela Politécnica de Cáceres.

Práctica 4. Auditoría de ciberseguridad holística empresarial

Sesión 2

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 proporcionalidad en la aplicación de la ciberseguridad. Se trata de reconocer que la ciberseguridad de un activo debe abordarse en proporción a la criticidad y el impacto de un posible incidente cibernético y comprender que esto no implica descuidar la protección.

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) ¿Cuál sería el número de funciones de ciberseguridad, categorías de ciberseguridad y actuaciones de ciberseguridad que potencialmente aplicarían a cada uno de los activos? 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. Describe el proceso seguido.

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

Ejercicio 2. A continuación, abre el caso *1_ Sesion_2_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 0.38702303. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas actuaciones de ciberseguridad que no se han implantado deben seguir sin implantarse.
- Aquellas actuaciones de ciberseguridad que se han implantado en algún grado pueden ampliarse, implementándolas en un grado mayor.
- El nivel global buscado, de ciberseguridad del activo de negocio, es de al menos 0.5.

a) Haz una captura de FLECO Studio, resaltando dónde se muestra el nivel global de ciberseguridad del activo de negocio.

b) 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_2_IG1_manual.fleco*.

c) 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_2_IG1.fleco*. Se corresponde con el mismo activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0.38702303 igual que en el ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas actuaciones de ciberseguridad que no se han implantado pueden implantarse total o parcialmente si es necesario.
- Aquellas actuaciones de ciberseguridad que se han implantado en algún grado no pueden modificarse. Seguirán implantadas en el mismo grado en el que lo están ya.
- El nivel global buscado, de ciberseguridad del activo de negocio, 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 *2_Sesion_2_IG1_manual.fleco*.

b) A la vista de lo realizado en este 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 4. A continuación, abre el caso *3_Sesion_2_IG1.fleco*. Se corresponde con el mismo activo de negocio de criticidad baja, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0.38702303 igual que en ejercicios anteriores. En este caso, no tiene objetivos/restricciones estratégicas de ciberseguridad definidas porque no es algo que vayamos a usar en este ejercicio.

Abre otra instancia de FLECO Studio y en él, crea un nuevo caso, para un activo de criticidad alta (grupo de implementación *IG3*); vamos a suponer que es el mismo activo, al que se le ha re-catalogado con una criticidad mayor por algún motivo. Ahora, replica en él los valores *Current status* del caso *3_Sesion_2_IG1.fleco*. Habrá muchas métricas CyberTOMP en este caso nuevo que no aparecen en el caso *3_Sesion_2_IG1.fleco*. Para esos casos, déjalos a cero. Cuando lo tengas todo replicado, guárdalo como *3_Sesion_2_IG1_manual.fleco*

a) Anota el valor del nivel global de ciberseguridad del activo en ambos casos. En el caso 3_Sesion_2_IG1.fleco era de 0.38702303, como hemos comentado; el del caso *IG3* que has creado y sobre el que has replicado los valores, debe ser distinto.

b) A la vista de lo realizado en este ejercicio, ¿has identificado algún efecto sobre el nivel de ciberseguridad global del activo con relación a su cambio de criticidad? ¿Por qué crees que esto es así?

Ejercicio 5. En la carpeta donde hayas guardado el fichero *3_Sesion_2_IG1_manual.fleco*, duplica este archivo y guarda la copia como *4_Sesion_2_IG1_manual.fleco*. Ahora desde FLECO Studio, abre el fichero *4_Sesion_2_IG1_manual.fleco*.

a) Modifica el valor *Current status* de cualquiera de las actuaciones de ciberseguridad hasta lograr un nivel de ciberseguridad global del activo similar al del *caso 3_Sesion_2_IG1.fleco*, es decir, similar a 0.38702303. Es muy difícil logar un valor exacto, pero uno aproximado sirve para lo que se pretende en este ejercicio. Guarda los cambios cuando lo hayas logrado.

b) Con este ejercicio has conseguido un nivel similar de ciberseguridad entre un activo y el mismo activo cuando se re-cataloga como de criticidad alta. Pero… ¿A costa de qué? ¿Qué has tenido que hacer para lograr el mismo nivel de ciberseguridad?

Al finalizar esta sesión deben quedar claras dos ideas:

1. La ciberseguridad es proporcional a la criticidad del activo de negocio y el impacto provocado por un ciberataque al mismo. Esto es lo que justifica una mayor dedicación de recursos.
2. La forma de aplicar un nivel de ciberseguridad mayor es: disponiendo de una mayor colección de actuaciones de ciberseguridad potencialmente aplicable; seleccionando un mayor número de ellas e implicando a más áreas; finalmente, implementándolas en un mayor grado.