Auditoría y Legislación Informática.

Escuela Politécnica de Cáceres.

Práctica 4. Auditoría de ciberseguridad holística empresarial

Sesión 3

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 ciberseguridad holística. Se trata de comprender la naturaleza holística de la ciberseguridad y entender la incapacidad de abordar eficazmente la ciberseguridad de un activo únicamente a través de un enfoque tecnológico.

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 áreas funcionales distintas y en cuantas ocasiones cada una podrían potencialmente contribuir a la ciberseguridad para 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 tercera columna de la aplicación. Anótalos. No es necesario guardar los casos.

b) ¿Qué relación observas entre el número distinto de áreas funcionales y el número de veces que cada una de ellas podría contribuir a la ciberseguridad del activo y el nivel de criticidad del activo? ¿Te parece razonable?

Ejercicio 2. A continuación, abre el caso 1_Sesion_3_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 0,23774332. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas áreas funcionales que todavía no están contribuyendo a la ciberseguridad del activo, deben seguir sin contribuir.
- Aquellas áreas funcionales que ya estén contribuyendo a alguna actuación de ciberseguridad, pueden seguir implementando en mayor profundidad esas mismas actuaciones o también contribuir a otras adicionales de las que estén bajo su área de responsabilidad, aunque las actuaciones de éstas aún no se hayan implementado en ningún grado.
- 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 *1 _Sesion_3_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_3_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 0,23774332. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas áreas funcionales que todavía no están contribuyendo a la ciberseguridad del activo, deben seguir sin contribuir.
- Aquellas áreas funcionales que ya estén contribuyendo a alguna actuación de ciberseguridad, pueden seguir implementando en mayor profundidad esas mismas actuaciones o también contribuir a otras adicionales de las que estén bajo su área de responsabilidad, aunque las actuaciones de éstas aún no se hayan implementado en ningún grado.
- 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 hayas terminado guárdalo como *2_Sesion_3_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_3_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 0,23774332. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas áreas funcionales que todavía no están contribuyendo a la ciberseguridad del activo, pueden comenzar a contribuir.
- Aquellas áreas funcionales que ya estén contribuyendo a alguna actuación de ciberseguridad, pueden seguir implementando en mayor profundidad esas mismas actuaciones o también contribuir a otras adicionales de las que estén bajo su área de responsabilidad. Es decir, tener una mayor contribución a la ciberseguridad del activo aprovechando que ya están implicadas.
- 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_3_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 los recursos que cada área debe emplear en la ciberseguridad del activo? ¿Están más o menos equilibrados? ¿Quién debería decidir qué posible combinación de áreas/actuaciones se implementa?

Ejercicio 5. A continuación, abre el caso *4_Sesion_3_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 0,23774332. Es el mismo caso del ejercicio anterior. Verás que tiene un único objetivo/restricción estratégica de ciberseguridad definida, consistente básicamente en:

- El nivel global buscado, de ciberseguridad del activo, es exactamente 1, 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_3_IG1_manual.fleco*.

b) A la vista de lo realizado en este 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 tres ideas:

1. El número de áreas funcionales que potencialmente tienen implicación en la ciberseguridad 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.
2. La forma de aplicar una ciberseguridad mayor es: que las áreas que ya participan en la ciberseguridad lo hagan de una forma más intensa (implementando un mayor número de sus acciones o las mismas, pero en un mayor grado) o involucrando a otras áreas que también tengan responsabilidad en la ciberseguridad del activo para que empiecen a contribuir desde su área de expertise. Lo primero tiene un alcance limitado mientras que lo último permite lograr incluso un nivel del 100% de ciberseguridad global del activo.
3. Cuando participa más de un área, éstas comparten tanto liderazgo como el conjunto de actuaciones a implementar por cada una, teniendo que consensuar el grado de implementación.