Auditoría y Legislación Informática.

Escuela Politécnica de Cáceres.

Práctica 4. Auditoría de ciberseguridad holística empresarial

Sesión 5

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 para comprender que el nivel de ciberseguridad de un activo fluctúa con el tiempo debido a factores tanto externos como internos, independientemente de la implementación de una serie de medidas de ciberseguridad multidisciplinarias, incluso si estas medidas permanecen sin cambios.

Ejercicio 1. Abre el caso *1_Sesion_5_IG3.fleco*. Se corresponde con un activo de negocio de criticidad alta, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,4164952. Como cada cierto tiempo, se evalúa que la ciberseguridad del activo no haya cambiado debido a factores internos o externos. En este caso, el equipo de trabajo multidisciplinar de ciberseguridad, en una de sus reuniones detecta que ha aumentado las repercusiones en la imagen de la organización y estima que el trabajo que se había realizado desde el área funcional *FA12 – Comunication and relationships* ha dejado de ser válido. No obstante, se desea mantener el mismo nivel de ciberseguridad para todas las métricas y también el mismo nivel de ciberseguridad global del activo. Por tanto, en este contexto:

a) Modifica manualmente los valores de *Current status* para expresar que los valores correspondientes a las actuaciones de ciberseguridad de la citada área bajan al nivel discreto de implementación anterior. Las actuaciones con valor de implementación 1.0 bajan a 0,67, las de 0,67 bajan a 0,33, las de 0,33 bajan a 0 y las de 0,0 se mantienen. Anota el nuevo nivel global de ciberseguridad actual del activo.

b) Crea restricciones/objetivos de ciberseguridad, ajustando los valores de las columnas *Constraint operator* y *Constraint value*, para todas las métricas, de formas que exprese que se desea mantener un valor exactamente igual al de la columna *Current status* original, antes de descender el activo global. Describe cómo lo has hecho.

c) Ejecuta FLECO de forma automática para que calcule una solución que permita cumplir con los objetivos marcados. Comprueba que es así y que en la columna *Target status* se obtiene el valor 0,4164952, manteniéndose por tanto el objetivo cumplido tal y como estaba. ¿Qué ha cambiado en la solución calculada por FLECO?

d) Guarda el caso como *1_Sesion_5_IG3_manual_automatico.fleco*.

e) A la vista de lo realizado en este ejercicio ¿Has entendido que, aunque no haya cambios en las medidas de seguridad implementadas, su validez puede variar simplemente porque varíe la naturaleza de la amenaza/riesgo? ¿En este caso, si tuvieras que resumir en una frase qué ha habido que hacer para mantener todo exactamente igual en términos de nivel de ciberseguridad, qué dirías? ¿Qué área funcional ha asumido el coste (en sentido amplio) de tener que mantener el mismo nivel de ciberseguridad cuando ha cambiado el contexto externo?

Ejercicio 2. Abre el caso *2_Sesion_5_IG3.fleco*. Se corresponde con un activo de negocio de criticidad alta, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,4164952. Como cada cierto tiempo, se evalúa que la ciberseguridad del activo no haya cambiado debido a factores internos o externo. En este caso, la alta dirección indica que la organización ha ganado un proyecto que va a imposibilitar que el área *FA7 – Risk assessment* pueda aportar nada a la ciberseguridad de dicho activo. Y el área *F09-Framework and standards* se tendrá que mantener aportando exactamente lo mismo, pero no más, porque también va a participar en dicho proyecto. No obstante, se desea mantener el mismo nivel de ciberseguridad global del activo. En este contexto:

a) Crea restricciones/objetivos de ciberseguridad, ajustando los valores de las columnas *Constraint operator* y *Constraint value*, de las funciones involucradas, de formas que exprese las restricciones que la alta dirección ha trasladado. Describe cómo lo has hecho.

b) Crea la restricción para el global del activo de negocio. Describe cómo lo has hecho.

c) Ejecuta FLECO de forma automática para que calcule una solución que permita cumplir con los objetivos marcados. Comprueba que es así y que en la columna *Target status* se obtiene el valor 0,4164952 o superior, manteniéndose por tanto el objetivo cumplido. ¿Qué ha cambiado en la solución calculada por FLECO?

d) Guarda el caso como *2_Sesion_5_IG3_manual_automatico.fleco*.

e) A la vista de lo realizado en este ejercicio, ¿Has entendido que por necesidades del negocio puede ser necesario que la participación de ciertas áreas en la ciberseguridad del activo se vea limitada? ¿En este caso, si tuvieras que resumir en una frase qué ha habido que hacer para mantener el nivel global de ciberseguridad del activo igual, qué dirías? ¿Qué áreas funcionales han asumido el coste de tener que mantener al menos el mismo nivel de ciberseguridad cuando ha cambiado el contexto externo?

Ejercicio 3. Abre el caso *3_Sesion_5_IG3.fleco*. Se corresponde con un activo de negocio de criticidad alta, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,4164952. Como cada cierto tiempo, se evalúa que la ciberseguridad del activo no haya cambiado debido a factores internos o externo. En este caso, la alta dirección indica que el activo, que anteriormente había sido catalogado como de criticidad alta, ahora pasa a ser catalogado como de criticidad media. Se desea mantener al menos el mismo nivel de ciberseguridad global del activo, no obstante. En este contexto:

a) Abre una nueva instancia de FLECO Studio, para un caso nuevo correspondiente al nivel de criticidad media (IG2). Traslada los valores de la columna *Current status* del caso original al nuevo caso que has creado. Habrá métricas que aplicaban al activo antes, cuando era de criticidad alta, pero ya no aplican con criticidad media. Esos valores, lógicamente, no tienes que trasladarlos. Asegúrate que, cuando lo tengas finalizado, el nivel global de ciberseguridad del activo es superior o igual a 0,4164952, el valor que tenía cuando estaba catalogado con mayor criticidad. Cuando lo tengas hecho, guárdalo como *3_Sesion_5_IG2_manual.fleco*.

b) A la vista de lo realizado en el ejercicio, ¿se comprende que la reclasificación del activo de negocio por parte de la organización implica que deben aplicársele más o menos actuaciones de ciberseguridad? Dependerá de si se clasifica con menor o mayor nivel. ¿En este caso, qué ha ocurrido con el nivel global de ciberseguridad del activo? ¿Y que significa que hubiera métricas que ya no aplican? ¿Qué pasa con esas áreas funcionales o las medidas que éstas habían implementado?

Ejercicio 4. A Abre el caso *4_Sesion_5_IG3.fleco*. Se corresponde con un activo de negocio de criticidad alta, de la citada organización. Su estado actual de ciberseguridad arroja un nivel de ciberseguridad global del activo de 0,24308446. Está protegido exclusivamente por el área tradicional más tecnológica, *FA10 – Security Architecture* que, por cierto, está bastante saturada con este activo. La alta dirección ha decidido implantar un modelo más holístico de la ciberseguridad por lo que pide que, para el siguiente año, la participación de esta área disminuya y participen al menos en algún aspecto el resto de las áreas, para que vayan participando en la ciberseguridad de la organización. Se desea incrementar el nivel de ciberseguridad global del activo al menos hasta el 0,4. En este contexto:

a) Utiliza las columnas *Constraint operator* y *Constraint value* para modelar lo que la alta dirección ha pedido. Ejecuta FLECO Studio para que, de forma automática, calcule un estado que cumpla con los objetivos definidos. Cuando lo tengas finalizado, guárdalo como *4_Sesion_5_IG3_manual_automatico.fleco*.

b) A la vista de lo realizado en el ejercicio, ¿se comprende que se puede mantener un mismo nivel de ciberseguridad involucrando a todas las áreas que pueden participar y de esta forma evitar la saturación de alguna de ellas? ¿Según el ejercicio, hubiera sido posible alcanzar el nivel de seguridad global solicitado por la alta dirección sólo con la participación del área funcional original? En cualquier caso, lográndose el mismo nivel de ciberseguridad ¿cuál crees que es la opción más holística y beneficiosa para la organización, aquella en la que participa una única área funcional o en la que participan todas?

Al finalizar esta sesión deben quedar claras dos ideas:

1. Existen factores internos y externos que hacen que la validez de la efectividad de las medidas implementadas varíe sin que la implementación de éstas haya variado. Es algo que hay que revisar constantemente y, aunque las actuaciones de ciberseguridad sean las mismas, su implementación habrá que adaptarla para cubrir las nuevas realidades. Cada área funcional debe asumir este papel para las actuaciones que le haya tocado implementar, de forma que son las encargadas de adaptar la ciberseguridad al contexto dinámico de ciberamenazas.
2. Siempre es mejor un enfoque holístico donde se integren distintas actuaciones de ciberseguridad de distintas áreas funcionales que aporten visiones distintas para el mismo objetivo de protección del activo. Esto permite a la organización una mayor maleabilidad, una mejor adaptación a circunstancias sobrevenidas en la organización, a no saturar y de pender exclusivamente de una o dos áreas funcionales y a mantener un enfoque cohesionado y de frente común ante las ciberamenazas.