Auditoría y Legislación Informática.

Tutorial sobre ciberseguridad holística.

Escuela Politécnica de Cáceres.

Ciberseguridad holística con *FLECO Studio*:
Fast, Lightweight, and Efficient Cybersecurity Optimization Studio.

Seguridad de las TIC → Seguridad de la información → Ciberseguridad

"Ámbitos cada vez más extensos. Cada vez más áreas implicadas. Cada vez menos control sobre el ecosistema. Cada vez más colaboración necesaria."

Ciberespacio: Conjunto de sistemas de información interconectados a través de redes de comunicación en las cuales las personas y entidades interactúan y llevan a cabo sus actividades. Posee características singulares: alto dinamismo; es un campo de juego común en el cual cada organización controla solo una parte y el resto depende de terceros; requiere que el enfoque se centre no tanto o no solo en la información, sino también en la continuidad de los procesos o activos empresariales; existe una necesidad de ciber-resiliencia; riesgos y amenazas específicas, etcétera.

Ciberseguridad: Única disciplina que permite abordar adecuadamente los riesgos, amenazas y situaciones derivadas de la existencia del ciberespacio y su relación con la organización.

Holismo: El holismo considera que el "todo" es un sistema más complejo que una simple suma de sus elementos constituyentes o, en otras palabras, que su naturaleza como ente no es derivable de sus elementos constituyentes. El holismo defiende el sinergismo entre las partes y no la individualidad de cada una [Wikipedia].

Una gestión holística de la ciberseguridad implica la acción común de toda la organización desde todas las áreas de expertise involucradas, mediante la unidad de acción de todas ellas. No hay ciberseguridad si ésta no es holística.

Se requiere un cambio de enfoque:

- ¿Quién es responsable de la ciberseguridad en un modelo holístico?

  Generalmente hay un área específica donde se ubica el CISO (Chief Information Security Officer), independiente del resto, que planifica e impulsa la ciberseguridad a alto nivel. Pero se requiere un liderazgo compartido por todas las áreas y departamentos.

- Si involucra a toda la organización, ¿esto significa que cada área funcional tiene responsabilidad en la ciberseguridad? ¿Cuál?

  La tiene. Lo habitual es que existan una serie de actuaciones de ciberseguridad específicas para cada área y no sólo para las más tecnológicas. Actuaciones en el ámbito jurídico, de recursos humanos, de comunicación, tecnológico, procedimental, de estándares, etcétera. Sólo piensa en cualquiera de los ciberataques más sonados en los últimos meses y en qué debería haberse hecho desde cualquiera de las áreas de la organización, antes, durante y después para evitarlo, minimizarlo, recuperarse del mismo (en todos los sentidos).

- ¿Hay que gestionar un equipo de trabajo multi-área donde cada área pertenece a un departamento? ¿Cómo se hace eso? ¿Cuál es la cadena de mando?

  Con mucha mano izquierda, con un enfoque al liderazgo compartido, superando los intereses exclusivos de cada unidad funcional, área o departamento. Y, sobre todo, delegando dicho liderazgo en la gestión en los niveles tácticos y operativos de la organización. Los encargados en primera persona de adaptar la organización al contexto de ciberamenazas del momento, cada uno desde su área de especialización. Obviamente, dotándoles de procesos, procedimientos y elementos metodológicos para ello.

CyberTOMP[1] Es un framework para la gestión holística de la ciberseguridad en niveles tácticos y operativos. Se centra en la protección de activos de negocio que son la unidad mínima de trabajo en las labores de ciberseguridad. Proporciona un listado unificado de actuaciones de ciberseguridad basado en diversos estándares

[1] 1 M. Domínguez-Dorado, J. Carmona-Murillo, D. Cortés-Polo and F. J. Rodríguez-Pérez, "CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels" in IEEE Access, vol. 10, pp. 122454-122485, 2022, doi: 10.1109/ACCESS.2022.3223440.

reconocidos. Los agrupa en tres niveles, IG1, IG2 e IG3, para ser aplicados a activos de negocio con requisitos bajos, medios o altos de ciberseguridad, respectivamente. Identifica todas las áreas de conocimiento de la organización implicadas en la ciberseguridad. Cada actuación del listado está asociada a una de ellas, la cual es la responsable principal de la misma.

Define niveles discretos de implementación que permiten describir sin ambigüedad el avance en la ejecución de cada una de las actuaciones. Las actuaciones están organizadas en categorías y funciones, en forma de árbol, dependiendo de la dimensión de la ciberseguridad a la que aportan.

Todas las actuaciones aplicables, junto con sus correspondientes niveles discretos de implementación, representan el estado de ciberseguridad del activo de negocio. Puede ser el estado actual (si se ha alcanzado dicho nivel de implementación) o el esperado, en caso contrario.

Partiendo de los niveles discretos de implementación de cada actuación de ciberseguridad, mediante un mecanismo de agregación, CyberTOMP proporciona métricas cuantitativas de la ciberseguridad del activo: por actuación de ciberseguridad, por cada categoría, por cada función, global del activo, etcétera. Y permite definir objetivos sobre dichas métricas.

Su característica más importante es que define los procesos, procedimientos y tareas que deben seguirse para lograr una gestión holística de la ciberseguridad desde los niveles tácticos y operativos de la organización. Esto es, define cómo deben colaborar y en qué momentos. El momento más crítico en dicha gestión holística, es llegar a un consenso sobre qué actuaciones de ciberseguridad hay que implementar y hasta qué nivel discreto de implementación cada una de ellas, como mínimo, para lograr los objetivos de ciberseguridad. Puede haber decenas de miles de posibilidades y cada una implica tareas, esfuerzo, costes, recursos técnicos y humanos… para las áreas que deben implementarlas.

Sin embargo, seleccionar las actuaciones de ciberseguridad que permitan alcanzar un estado de ciberseguridad del activo compatible con los objetivos estratégicos marcados no es nada sencillo. Hacerlo de una forma consensuada entre todas las áreas implicadas, lo hace aún más complicado.

Incluso las áreas más tecnológicas tienen dificultades para identificar la contribución específica que se requiere desde otras áreas funcionales para la ciberseguridad. Es imposible aportar a algo que desconoces que requiere tu implicación. Por tanto, la toma de decisiones en el ámbito táctico-operativo no es habitual. Estos niveles de la organización necesitan ser capaz de reconocer el contexto de ciberseguridad, de forma conjunta, y tomar una decisión acertada en un breve espacio de tiempo. Necesitan, resumiendo, reforzar su habilidad en conciencia situacional.

FLECO Studio es una plataforma que permite identificar de forma rápida conjuntos de actuaciones de ciberseguridad, y sus niveles discretos de implementación, que cumplan con los objetivos estratégicos marcados, para ser discutidos y acordados, si es su caso, por el equipo multidisciplinar de ciberseguridad.

Al mismo tiempo permite entrenar y reforzar las capacidades de conciencia situacional del equipo de trabajo, para habilitarles para tomar decisiones acertadas en la gestión de holística de la ciberseguridad desde su posición táctico-operativa.

Se ejecuta de forma sencilla con Java:

```
java -jar fleco-1.4-with-dependencies.jar
```

Tiene una interfaz sencilla, todas las opciones se encuentran en el menú y en la barra de herramientas (Fig. 1).

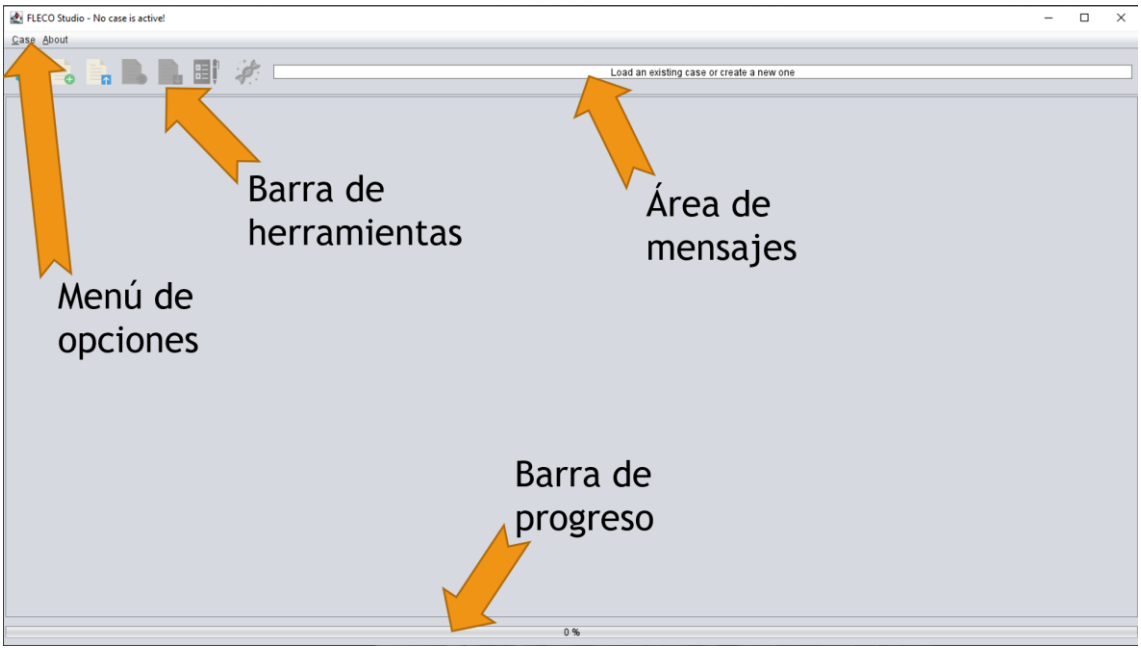

Figura 1. Interfaz principal de FLECO Studio. Fuente: CyberTOMP.

Opción Nuevo caso:

- Con la opción “Nuevo” (caso vacío).
- Con la opción “Random” (caso con datos aleatorios, para pruebas).

En ambos casos hay que elegir primero el grupo de implementación a aplicar: IG1, IG2 o IG3, para activos catalogados como de nivel BAJO, MEDIO o ALTO, respectivamente (Fig. 2).

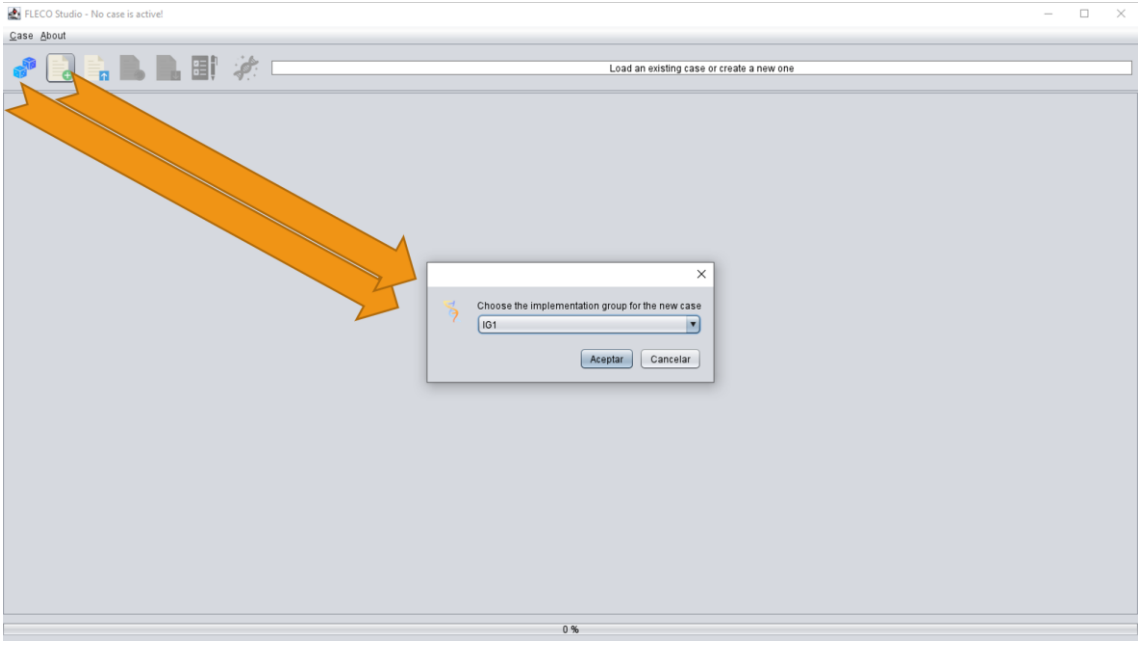

Figura 2. Generando un nuevo caso en la interfaz principal. Fuente: CyberTOMP.

Interfaz modo tabla (Fig. 3):

- Se debe trabajar de izquierda a derecha.

- Hay columnas editables. Doble clic en cualquiera de las tres primeras columnas abre una ventana con información extra sobre la métrica.

- Descripción de cada columna:
  - "CyberTOMP metric": cada una de las actuaciones de ciberseguridad disponibles según el IG elegido. Jerarquía en forma de árbol.
  - "Purpose": Objetivo de cada una de las métricas disponibles para el IG seleccionado.
  - "Leading functional área": Indica cuál es el área de expertise o área funcional de la organización que debe liderar la implementación de las actuaciones necesarias para cada métrica.
  - "Current status": columna editable (sólo para las métricas de más bajo nivel). Se debe indicar el Nivel Discreto de Implementación (NDI) para cada actuación de ciberseguridad. Las métricas se agregan y propagan hacia arriba automáticamente: categorías, funciones y activo. Significado de cada NDI:
    - ✓ 0.0: Ninguna de las sub-actuaciones que componen la actuación de ciberseguridad se ha implantado.
    - ✓ 0.33: Se han implementado varias sub-actuaciones de las que componen la actuación de ciberseguridad, pero menos de la mitad.

- ✓ 0.67: Se han implementado la mitad o más de las sub-actuaciones de las que componen la actuación de ciberseguridad, pero no todas.
- ✓ 1.00: Todas las sub-actuaciones que componen la actuación de ciberseguridad se han implementado.

- "Constraint operator": Columna editable a todos los niveles. Permite definir un objetivo/restricción sobre la métrica seleccionada (o es obligatorio definir un objetivo para cada métrica).
- "Constraint value": Permite definir el valor específico asociado al operador.
- "Target status": En esta columna *FLECO Studio* sugiere valores específicos de implementación de cada actuación de ciberseguridad que cumplen con los objetivos estratégicos definidos (Fig. 4). Sólo para el modo "Automático/Guiado".

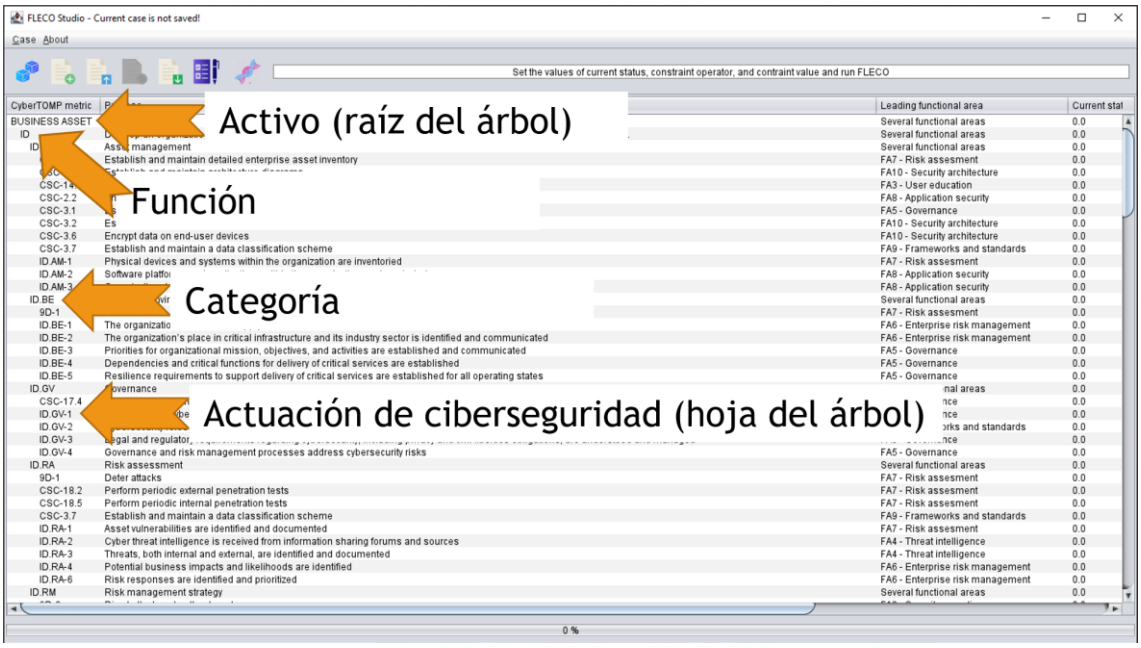

Figura 3. Interfaz modo tabla. Fuente: CyberTOMP.

Una vez definido completamente el "Current status" de ciberseguridad para el activo hay dos formas de trabajar:

- Manual: Se puede jugar con la columna "Current Status" hasta que se consiga cumplir con todos los objetivos/restricciones de ciberseguridad, cosa que se podrá detectar de forma visual al tener dichos objetivos definidos en las dos siguientes columnas. Cuando esto se logre, se habrá identificado un conjunto de actuaciones de ciberseguridad, así como los niveles discretos de implementación de cada una de ellas, que permiten lograr los objetivos deseados. Si hay consenso por parte de todas las áreas

funcionales implicadas, esto será el principio del plan de ciberseguridad del activo.

- Automático/Guiado (Fig. 4): *FLECO Studio* puede calcular de manera rápida y automática el citado conjunto de actuaciones de ciberseguridad de forma que sólo haya que consensuar entre todas las áreas que se está de acuerdo, o, si no se consigue acuerdo, volver a calcular otro.

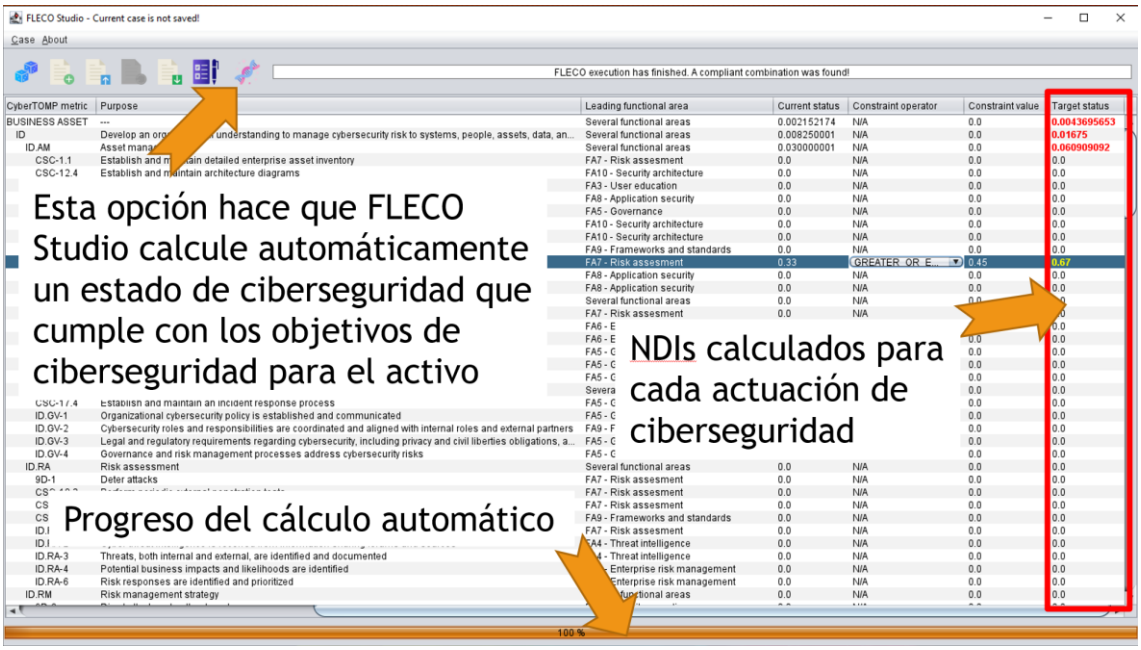

Figura 4. Modo de funcionamiento Automático/Guiado. Fuente: CyberTOMP.

Por último, el caso de estudio se puede guardar, recuperar de disco o actualizarlo con los últimos cambios realizados (Fig. 5).

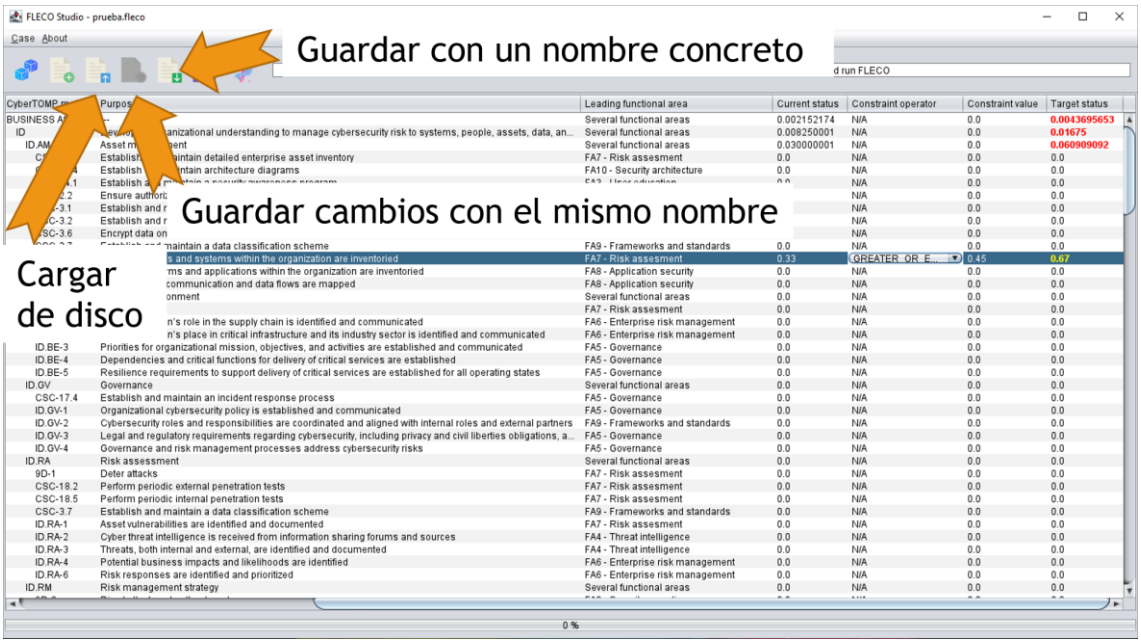

Figura 5. Opciones de importación/exportación de casos. Fuente: CyberTOMP.

Ejercicios:

1. Desarrolla un manual de usuario de la herramienta de gestión holística de ciberseguridad FLECO Studio (Fast, Lightweight, and Efficient Cybersecurity Optimization Studio).

2. Describe las características principales de la licencia de FLECO Studio.

3. Licencia el manual de usuario, seleccionando la licencia Creative Commons adecuada:
   https://chooser-beta.creativecommons.org/

4. Justifica y describe las características principales de la licencia escogida.