Manual de Fleco Studio

Realizado por Guadalupe Gónzalez Santos y José Antonio Bravo Romero.
Fecha de finalización: 08/12/2024.
Destinatario: futuros alumnos de ALI.

ÍNDICE

Conceptos.....3
Interfaz.....4
Creación de Casos.....5
Crear un nuevo caso vacío.....5
Crear un nuevo caso aleatorio.....6
Cargar un caso ya existente.....6
Estructura de los Casos.....7
Activo.....8
Función.....8
Categoría.....9
Actuación.....9
CyberTOMP metric.....10
Purpose.....11
Leading functional area.....11
Current status.....12
Constraint operator.....12
Constraint value.....13
Target status.....13
Características de la licencia de FLECO Studio.....15
Licencia.....15
Justificación.....16
Referencias Webgráficas.....16

Conceptos

Apartado en el que se aglutinan términos que son necesarios para entender el manual, además de su importancia por su uso repetitivo en éste.

Activo: conjunto de datos que reflejan la situación de una empresa en cuanto a su nivel de ciberseguridad.

Actuación: tarea específica de ciberseguridad.

Área Funcional: sector de la empresa al que se le asignan actuaciones de ciberseguridad que deben llevar a cabo

Categoría: conjunto de actuaciones, dedicadas a la misma función, que se relacionan entre ellas por llevar a cabo una tarea similar. Al juntar todas las categorías dentro de una función se suplen todas las necesidades de esa función.

Ciberseguridad: conjunto de métodos y técnicas que permiten proteger datos y archivos informáticos.

Criticidad: nivel de riesgo de ataque de ciberseguridad sobre los datos de la empresa.

Función: método de categorización que se usa para separar las distintas actuaciones de seguridad.

Grupo de implementación: categorización que agrupa a activos (IG<**nivel**>) dependiendo del nivel de peligro en el que se encuentre este.

Nivel de ciberseguridad global: qué porcentaje de los datos están asegurados y protegidos y qué cantidad de seguridad se está tomando sobre ellos.

Interfaz

Figura 1. Diferentes botones de la barra de herramientas.

- El **botón 1** sirve para generar un caso aleatorio con el que probar y aprender con diferentes valores de estado actual (Current status).
- El **botón 2** se utiliza para generar un nuevo caso, pero esta vez 'vacío', quiere decir, que todos los valores de la columna Current status están a 0.
- El **botón 3** se utiliza para cargar un caso previamente guardado .fleco
- El **botón 4** sirve para guardar los cambios realizados en un caso en el que está guardado.
- El **botón 5** se utiliza para guardar el caso, seleccionando un nombre y una localización en el ordenador.
- El **botón 6** pone el estado de ciberseguridad del activo mínimo para superar el cómputo puesto en la columna Target status.
- El botón **Case**: aglutina todos las funciones de los botones anteriormente explicados.
- El botón **About**: tiene dos secciones, una que te redirige al repositorio de Fleco Studio, mientras que la otra te permite ver la licencia del programa.

Creación de Casos

En este apartado se explicará las diferentes maneras de crear un nuevo caso en Fleco Studio. Se nos ofrecen 3 opciones:

- Crear un nuevo caso vacío
- Crear un nuevo caso aleatorios
- Cargar un caso ya existente

Crear un nuevo caso vacío

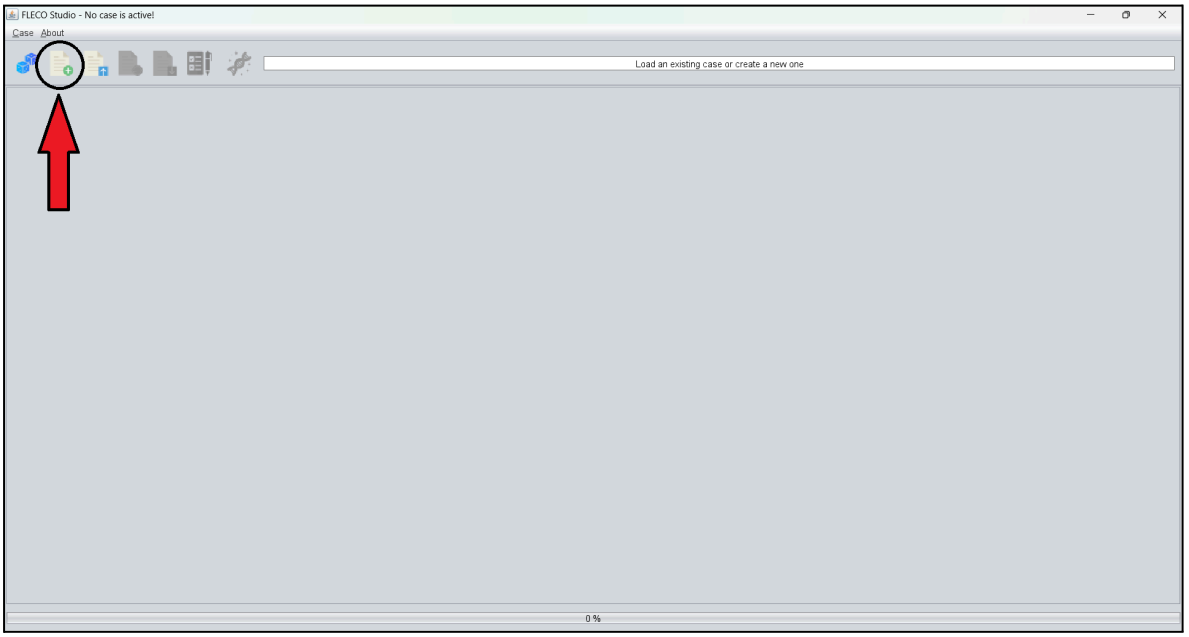


Figura 2. Creación de un nuevo caso vacío

Al pulsar el botón señalado en la Figura 2 se nos permite crear un caso vacío. Esto significa que se nos mostrarán todas las actuaciones que se pueden aplicar sobre el modelo de negocio, pero todas ellas estarán inicialmente con un valor 0.

Antes de crear el caso se nos pedirá que elijamos el nivel de criticidad del caso mediante la siguiente ventana:

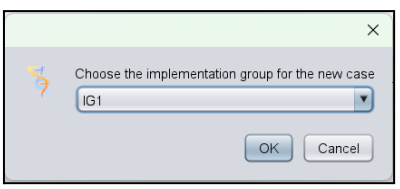


Figura 3. Selección del nivel de criticidad del activo

Crear un nuevo caso aleatorio

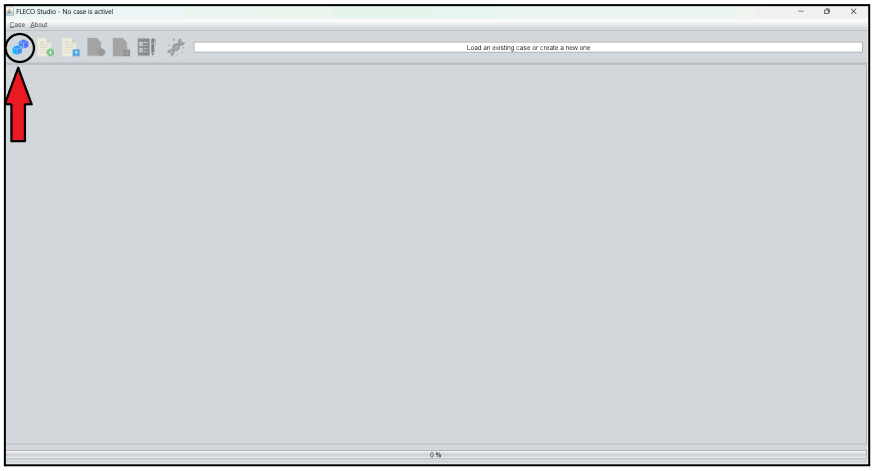


Figura 4. Creación de un caso aleatorio

Esta opción nos permite crear un nuevo caso que, al contrario que la opción anterior, se nos rellenará con valores aleatorios. Esto quiere decir que cada una de las actuaciones tendrá un porcentaje de actuación aleatorio.

De igual manera que en la opción anterior, antes de crear el caso se nos dará a elegir cuál queremos que sea el nivel de criticidad mediante la misma ventana.

Cargar un caso ya existente

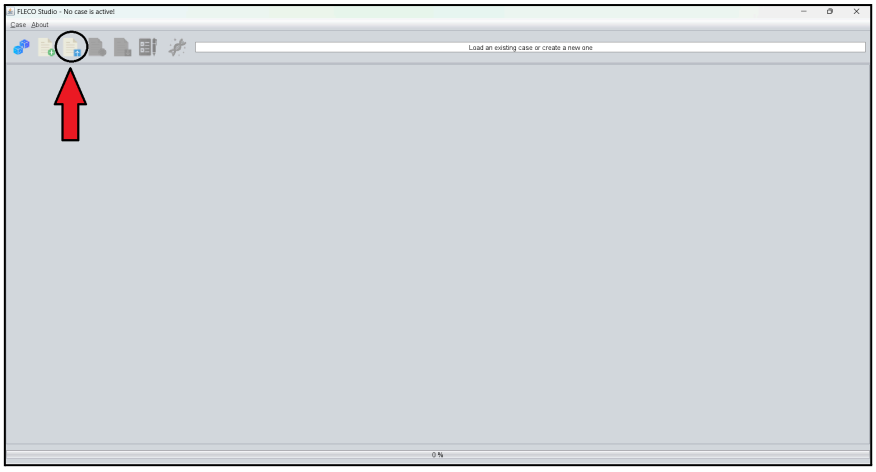


Figura 5. Cargar un caso ya existente

Esta opción nos permite cargar un caso ya existente dentro de nuestro espacio de trabajo de Fleco Studio. Esto significa que se cargará con el mismo nivel de criticidad y los mismos valores que ya posea.

Debido a esto, en esta opción no se mostrará ventana de elección de nivel de criticidad, ya que se mantiene el propio del caso.

Estructura de los Casos

Una vez creado el caso, se nos muestran los campos que reflejan la organización de un método de ciberseguridad de una empresa. Esto se ve como lo siguiente:

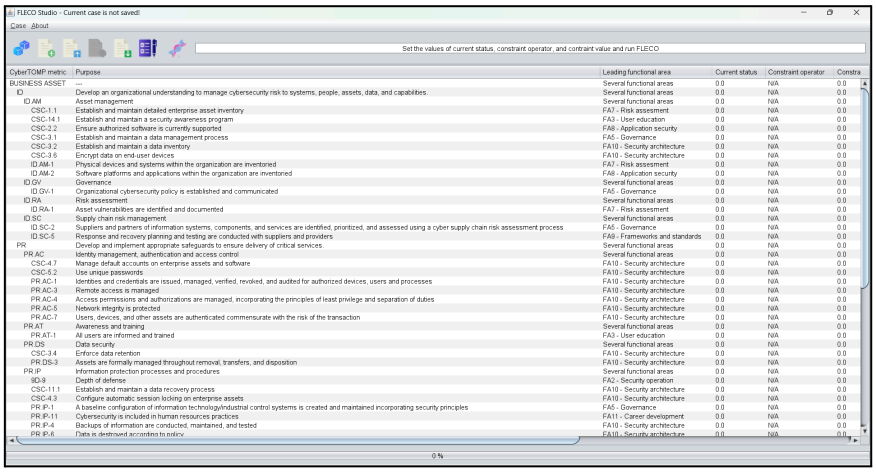


Figura 6. Primer vistazo de un caso aleatorio

El caso se organiza en filas y columnas. En primer lugar explicaremos las filas.

Entre las líneas debemos diferenciar 4 tipos diferentes:

- Activo
- Función
- Categoría
- Actuación

Activo

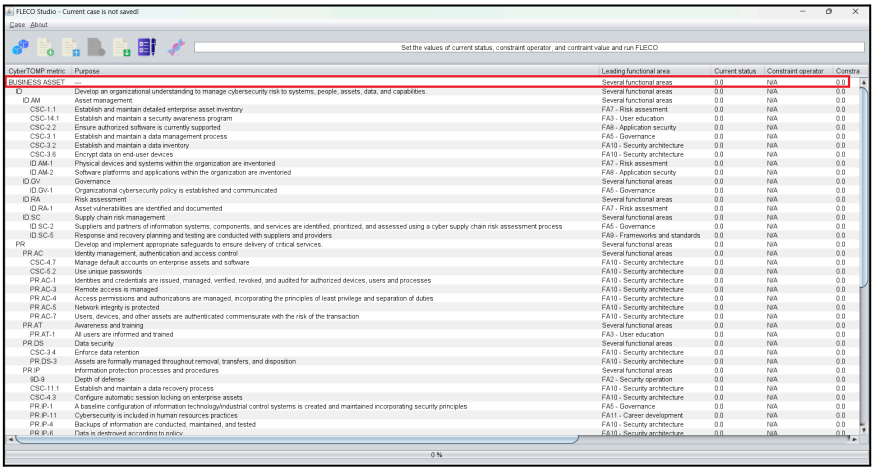


Figura 7. Análisis de la fila BUSINESS ASSET

En esta fila se especifica el resumen global de todo el caso, es decir, el nivel global de ciberseguridad del negocio.

Función

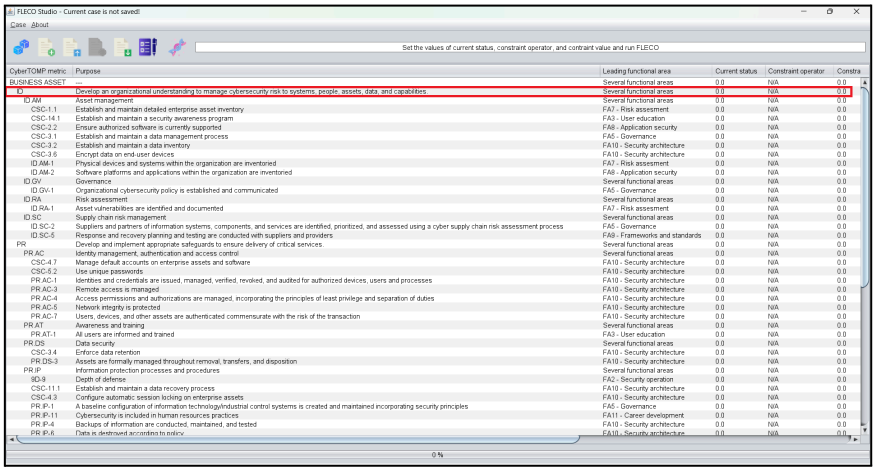


Figura 8. Análisis las funciones de un activo

La siguiente línea define las funciones principales en las que se divide la ciberseguridad de un activo. Hay un total de 4, independientemente del nivel de criticidad, y estas son identificación (ID), protección (PR), detección (DE) y responder (RS). Además, cuando el nivel de criticidad es de 3, se añade una función más: recuperar (RC).

Los valores de estas filas no pueden editarse manualmente, se calculan uniendo los resultados de sus categorías.

Categoría

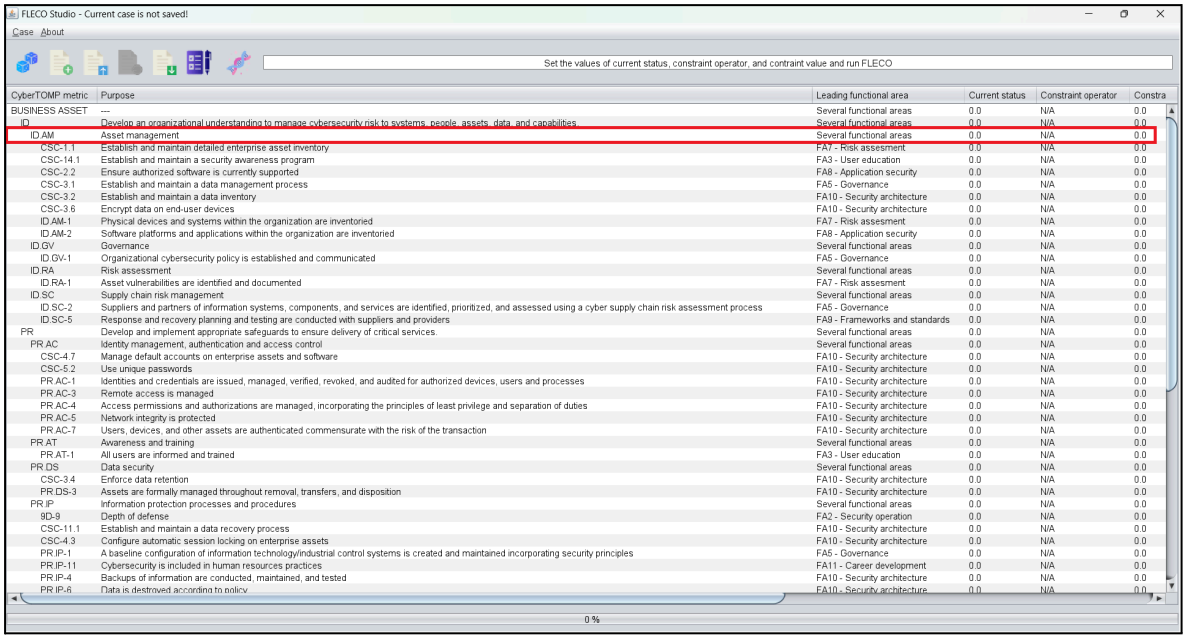


Figura 9. Análisis las categorías de un activo

Estas filas se usan como una manera de agrupar tareas dentro de una función. El número varía dependiendo de la función y del nivel de criticidad. Al igual que con las funciones, sus valores no pueden cambiarse manualmente, se calculan con respecto a sus tareas asociadas.

Actuación

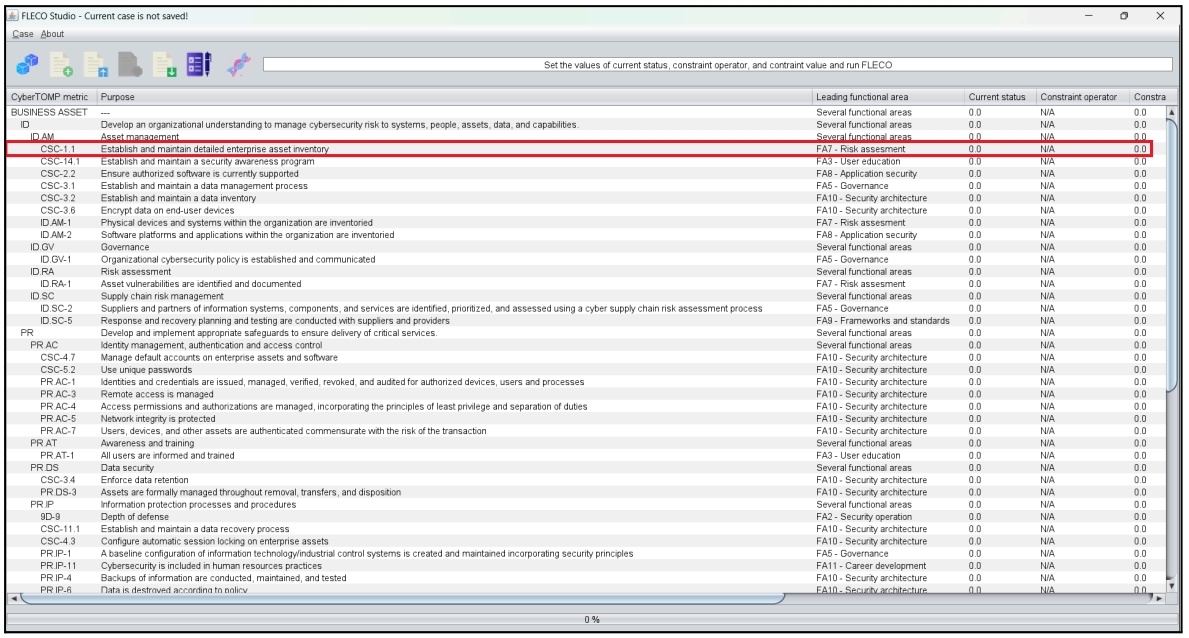


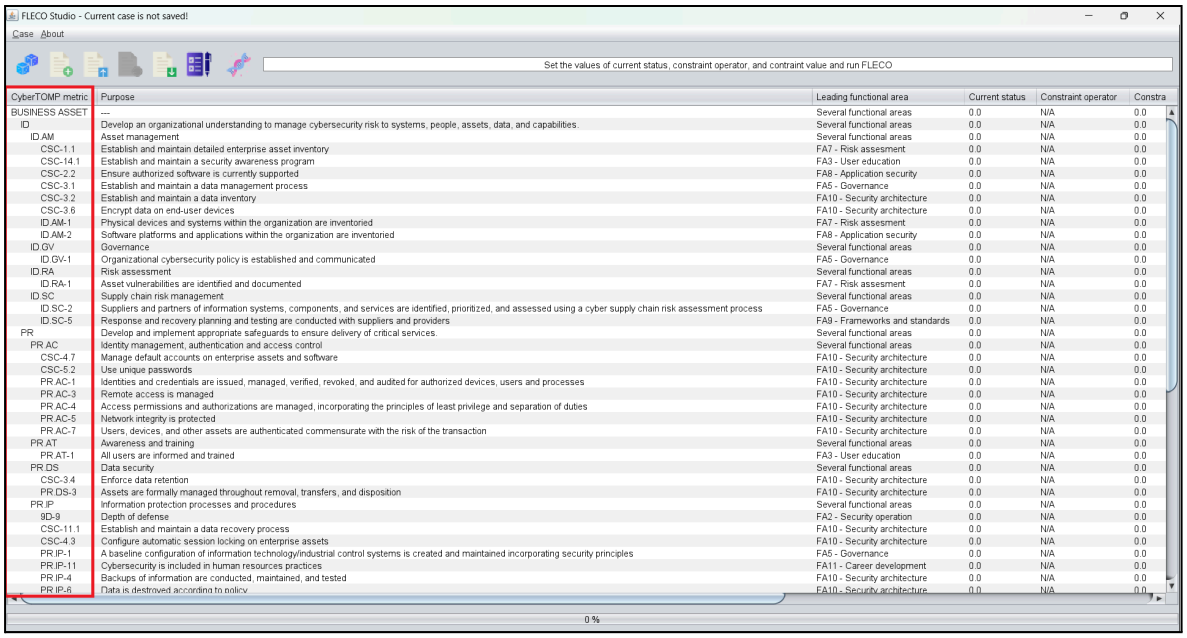
Figura 10. Análisis las actuaciones de ciberseguridad de un activo

Estas filas representan cada una de las tareas individuales que se deben llevar a cabo para reforzar la ciberseguridad de un activo. Sus valores se deben modificar para aumentar el nivel

de actuación, es decir, en qué porcentaje se desea que se supla la tarea en específico. Estos valores se explicarán en la explicación de la columna current status.

Una vez explicadas las diferentes filas, pasaremos a **explicar las columnas**:

CyberTOMP metric



CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constra
BUSINESS ASSET	---	Several functional areas	0.0	N/A	0.0
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.0	N/A	0.0
ID.AM	Asset management	Several functional areas	0.0	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assesment	0.0	N/A	0.0
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	0.0	N/A	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.0	N/A	0.0
CSC-3.1	Establish and maintain a data management process	FA5 - Governance	0.0	N/A	0.0
CSC-3.2	Establish and maintain a data inventory	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	0.0	N/A	0.0
ID.AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assesment	0.0	N/A	0.0
ID.AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.0	N/A	0.0
ID.GV	Governance	Several functional areas	0.0	N/A	0.0
ID.GV-1	Organizational cybersecurity policy is established and communicated	FA5 - Governance	0.0	N/A	0.0
ID.RA	Risk assessment	Several functional areas	0.0	N/A	0.0
ID.RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assesment	0.0	N/A	0.0
ID.SC	Supply chain risk management	Several functional areas	0.0	N/A	0.0
ID.SC-2	Suppliers and partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	FA5 - Governance	0.0	N/A	0.0
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA9 - Frameworks and standards	0.0	N/A	0.0
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.0	N/A	0.0
PR.AC	Identity management, authentication and access control	Several functional areas	0.0	N/A	0.0
CSC-4.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
CSC-5.2	Use unique passwords	FA10 - Security architecture	0.0	N/A	0.0
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	FA10 - Security architecture	0.0	N/A	0.0
PR.AC-3	Remote access is managed	FA10 - Security architecture	0.0	N/A	0.0
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	FA10 - Security architecture	0.0	N/A	0.0
PR.AC-5	Network integrity is protected	FA10 - Security architecture	0.0	N/A	0.0
PR.AC-7	Users, devices, and other assets are authenticated commensurate with the risk of the transaction	FA10 - Security architecture	0.0	N/A	0.0
PR.AT	Awareness and training	Several functional areas	0.0	N/A	0.0
PR.AT-1	All users are informed and trained	FA3 - User education	0.0	N/A	0.0
PR.DS	Data security	Several functional areas	0.0	N/A	0.0
CSC-3.4	Enforce data retention	FA10 - Security architecture	0.0	N/A	0.0
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	FA10 - Security architecture	0.0	N/A	0.0
PR.IP	Information protection processes and procedures	Several functional areas	0.0	N/A	0.0
9D-9	Depth of defense	FA2 - Security operation	0.0	N/A	0.0
CSC-11.1	Establish and maintain a data recovery process	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.3	Configure automatic session locking on enterprise assets	FA10 - Security architecture	0.0	N/A	0.0
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA5 - Governance	0.0	N/A	0.0
PR.IP-11	Cybersecurity is included in human resources practices	FA11 - Career development	0.0	N/A	0.0
PR.IP-4	Backups of information are conducted, maintained, and tested	FA10 - Security architecture	0.0	N/A	0.0
PR.IP-6	Data is destroyed according to policy	FA10 - Security architecture	0.0	N/A	0.0

Figura 11. Análisis la columna CyberTOMP metric

Esta columna muestra el acrónimo de la línea, ya sea el activo, una función, la categoría o una actuación.

Purpose

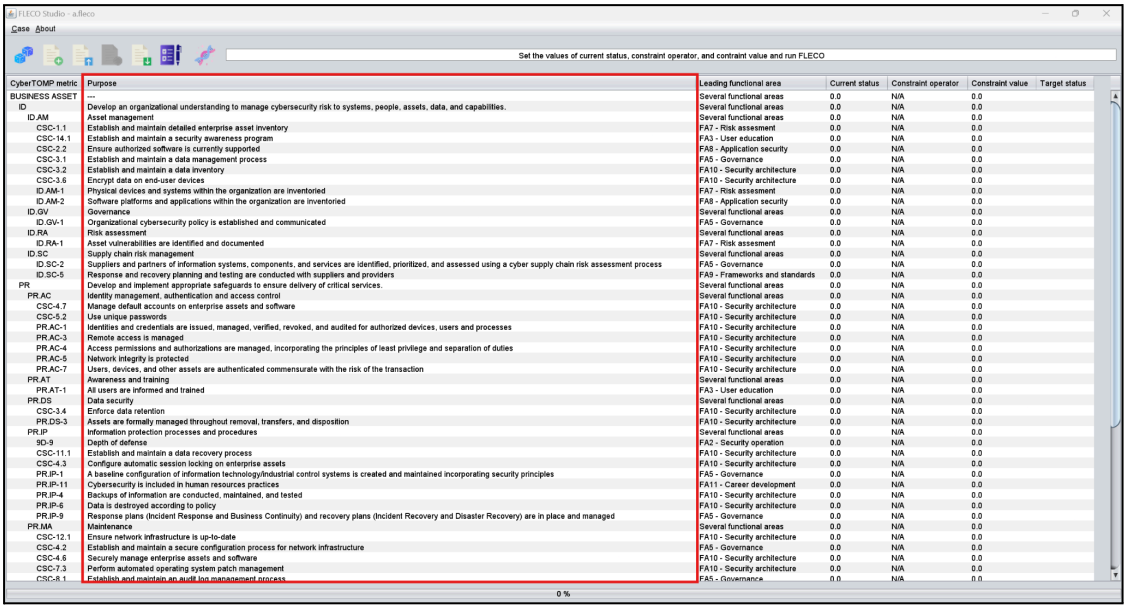


Figura 12. Análisis la columna Purpose

Esta columna muestra el propósito de la fila, es decir, para qué sirve o cuál es su tarea principal.

Leading functional area

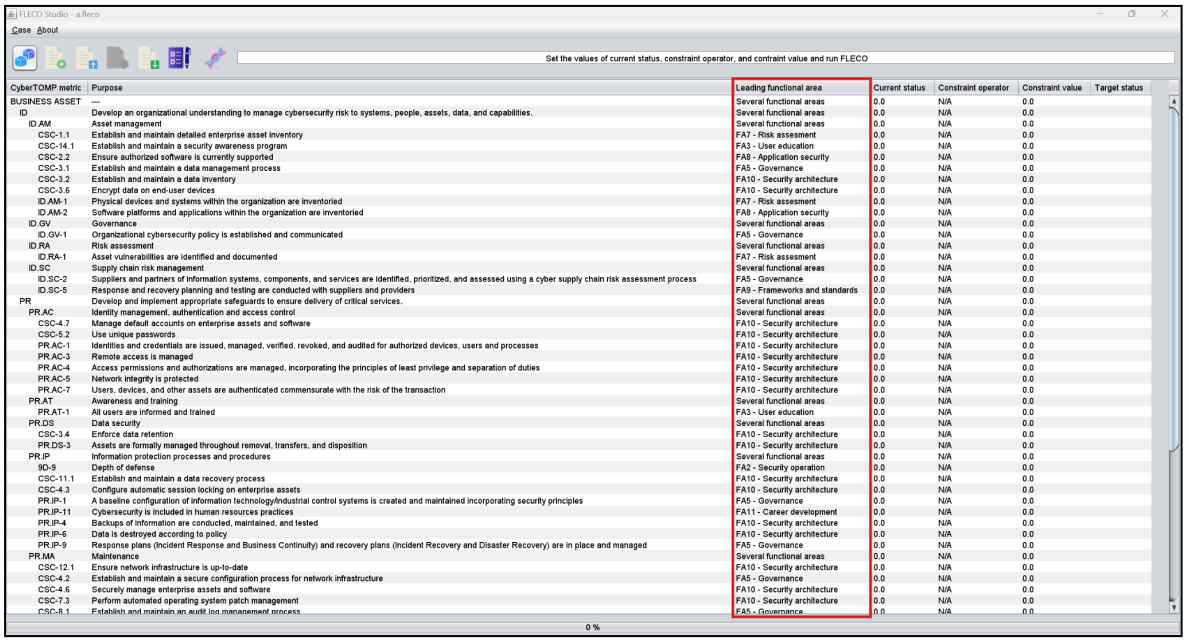


Figura 13. Análisis la columna Leading functional area

Esta columna muestra a qué área funcional está asignada la fila. En caso de que se trate de una actuación, debe salir una sola área funcional (FA2, FA10, etc). Si en vez de aparecer una área funcional aparece “several functional areas”, significa que hay varias áreas encargadas de la realización de esa fila.

Current status

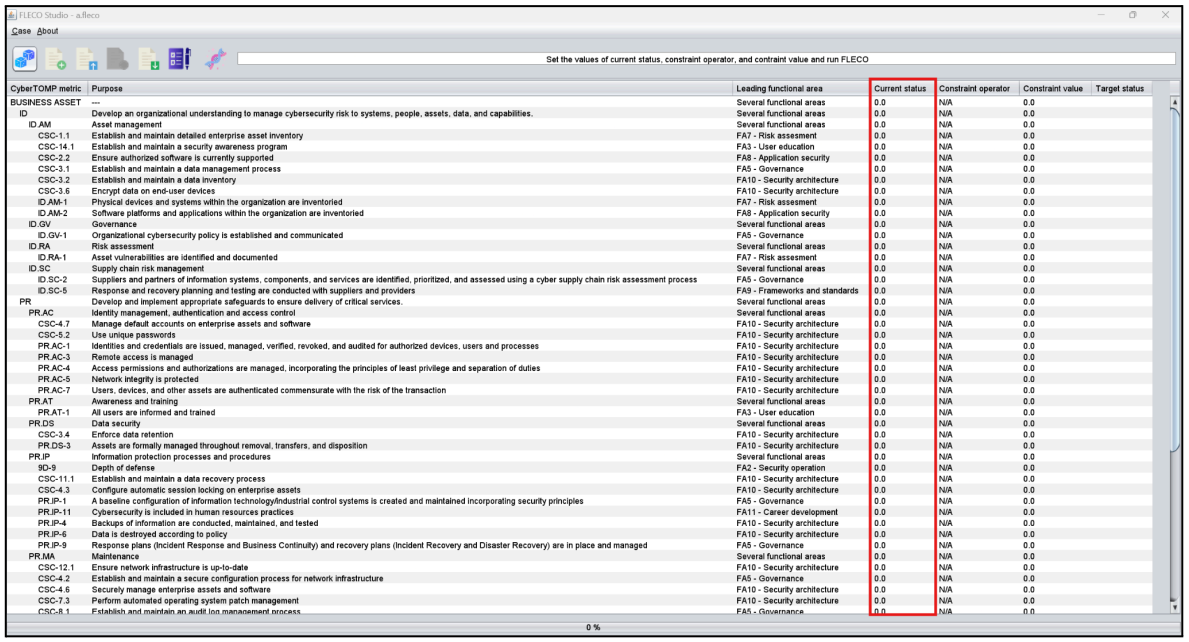


Figura 14. Análisis la columna Current status

Esta columna muestra el estado actual en el que se encuentra la fila, es decir, el porcentaje en el que se está aplicando. Este valor puede ser 0 (no se está aplicando), 0,33, 0,67, 1 (está al máximo).

Constraint operator

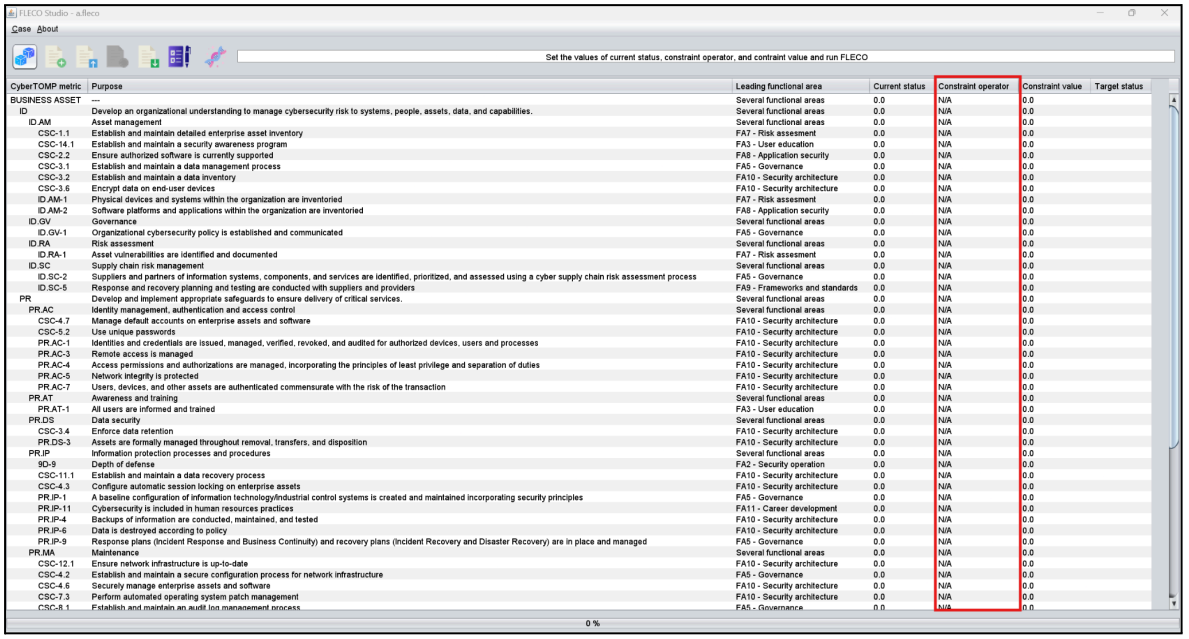


Figura 15. Análisis la columna Constraint operator

En esta columna se determinan los requisitos que se imponen a las filas, es decir, se aplica un operador (igual a, mayor o igual a, menor que…) con respecto a la columna “constraint value”. Si no hay ningún requisito, se establece el operador N/A.

Constraint value

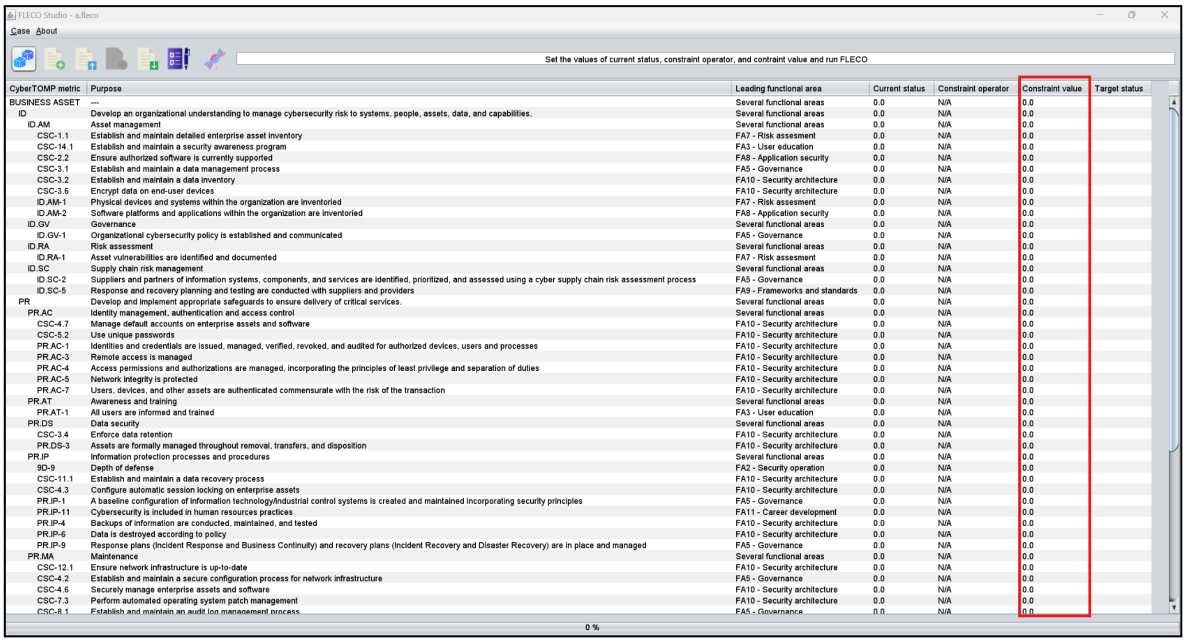


Figura 16. Análisis la columna Constraint value

En esta columna se especifica el valor sobre el que se aplicará el operador de la columna "constraint operator". Si no hay ningún operador establecido (N/A), el valor será 0, y no se permitirá su modificación.

Target status

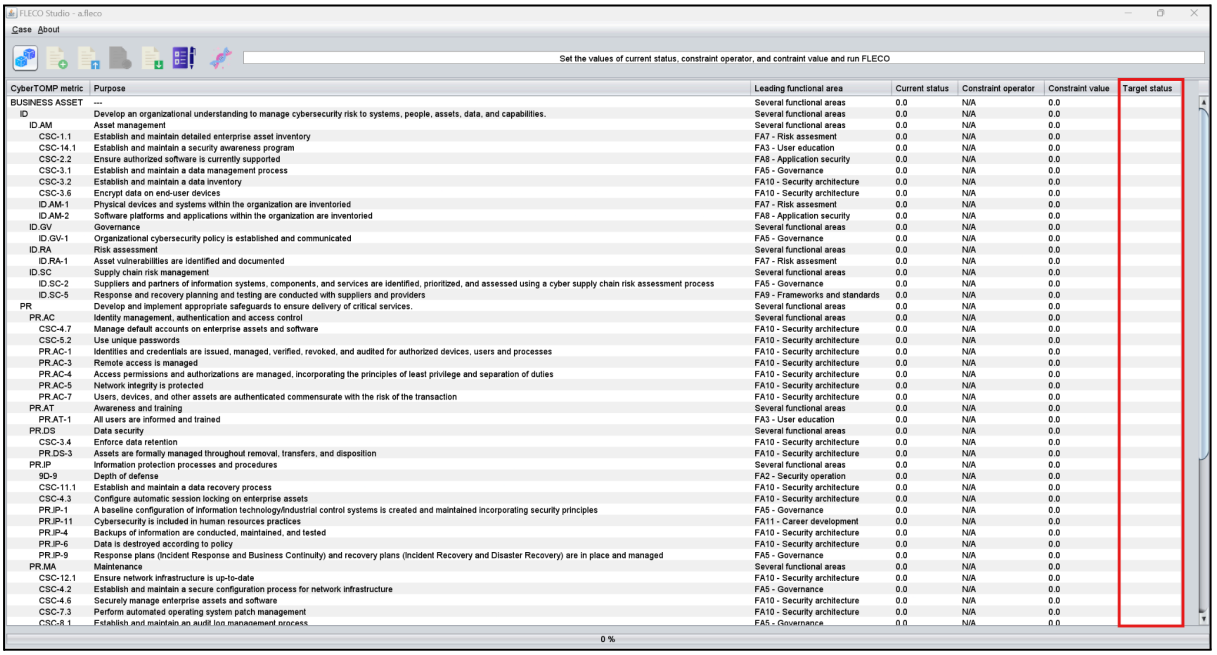


Figura 17. Análisis la columna Target status

Columna que establece el valor objetivo para llegar en la columna "constraint status".

Atajos

A continuación, se completa este apartado ya que se considera que aporta una serie de funciones, para el usuario, de gran utilidad :

1. **ctrl + N** ⇒ nuevo caso.
2. **ctrl + R** ⇒ nuevo caso random.
3. **ctrl + A** ⇒ seleccionar todo.
4. **ctrl + I** ⇒ ver licencia.
5. **F1** ⇒ sobre FLECO
6. Con una fila seleccionada, si se hace doble click con el click derecho en cualquier parte de la pantalla se abre el descriptor.
7. Con las flechas arriba y abajo, te permite moverte entre las diferentes filas.
8. Con el tabulador y las flechas derecha e izquierda, te mueves entre las columnas.
9. Dentro del descriptor no se te permite copiar de un solo golpe cada apartado, si se usa el **ctrl + A** se seleccionará sólo el párrafo que se encuentre seleccionado.
10. Con el ratón haciendo click y deslizando se pueden seleccionar las filas que se deseen.

Características de la licencia de FLECO Studio

La **GNU Lesser General Public License (LGPL) v3** se caracteriza por permitir el uso, la modificación y la distribución de software libre, enfocándose principalmente en bibliotecas con la posibilidad de vincular éstas con software propietario, siempre y cuando se salvaguarden las condiciones especificadas del software original. Esto se extiende también a aplicaciones, asegurando la posibilidad de cambio de las bibliotecas. En el caso de obras combinadas, se exige incluir previo aviso del uso de estas bibliotecas, proporcionando código fuente y garantizar la compatibilidad de interfaces con versiones posteriores modificadas.

Además, toda modificación realizada a una biblioteca, debe cumplir con las condiciones de la LGPL o la GLP, permitiendo elegir entre la versión de la LGPL bajo la cuál se recibió la biblioteca o cualquiera de sus versiones posteriormente publicadas por la Free Software Foundation

Licencia

Justificación

La elección de la licencia **CC BY-SA 4.0** refleja nuestra creencia sobre la libre difusión del conocimiento para los estudiantes de los años venideros, preservando al mismo tiempo nuestro reconocimiento sobre este manual. Así mismo, esta licencia permite ser compartida, copiada, adaptada, siempre y cuando se otorgue el crédito necesario a nuestra autoría y la distribución de obras derivadas bajo la misma licencia; promoviendo la colaboración e, incluso, el intercambio de ideas, salvaguardando los principios interpuestos de este nuestro proyecto -asegurando principios como el libre acceso y la contribución mútua-

Referencias Webgráficas

1. **GitHub - Fleco License**
   Manolodd. (s.f.). Fleco License. Consultado el 05-12-2024 de https://github.com/manolodd/fleco/blob/development/LICENSE

2. **Creative Commons - Share Your Work**
   Creative Commons. (s.f.). Share Your Work: CC Licenses. Consultado el 06-12-2024 de https://creativecommons.org/share-your-work/cclicenses/

3. **GNU Philosophy**
   Free Software Foundation. (s.f.). The Free Software Philosophy. Consultado el 07-12-2024 de https://www.gnu.org/philosophy/philosophy.html

4. **GNU Licenses**
   Free Software Foundation. (s.f.). GNU Licenses. Consultado el 08-12-2024 de https://www.gnu.org/licenses/licenses.html