

FLECO

SESIÓN 1

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

Introducción:

A) Descripción general de FLECO Studio:

-FLECO Studio es una herramienta de gestión holística de ciberseguridad diseñada para proporcionar una solución integral para la protección de activos digitales y la administración de riesgos. Este software combina eficiencia y velocidad con una interfaz intuitiva, permitiendo a los profesionales de ciberseguridad y a los administradores de sistemas mantener un control completo sobre la seguridad de la red y los activos críticos.

Características principales:

-Escaneo y Evaluación: FLECO Studio despliega herramientas de escaneo potentes, destinadas a identificar vulnerabilidades en sistemas, aplicaciones y redes. Asimismo, facilita la evaluación de riesgos, permitiendo la priorización de acciones de mitigación.

-Monitorización en Tiempo Real: La capacidad de monitorización en tiempo real capacita a los usuarios para recibir alertas inmediatas ante posibles amenazas y posibilitando respuestas rápidas y efectivas.

-Gestión de Activos: Facilitando la eficiente gestión y registro de activos digitales, FLECO Studio contribuye al mantenimiento de un inventario actualizado y a la aplicación de políticas de seguridad específicas.

-Herramientas Integradas: FLECO Studio abraza una gama completa de herramientas de seguridad, desde firewalls hasta análisis de vulnerabilidades, dotando a los usuarios de recursos amplios para salvaguardar la integridad y confidencialidad de sus sistemas.

B) Propósito del Manual:

-El propósito de este manual es ofrecer una guía meticulosa y completa sobre el uso efectivo de FLECO Studio. Concebido con la misión de allanar el terreno para la comprensión ágil y la adopción rápida de la herramienta, este manual propulsa a los usuarios hacia la maximización de sus capacidades en el fascinante dominio de la ciberseguridad.

REQUISITOS PREVIOS

Para utilizar FLECO Studio, necesitará los siguientes requisitos previos:

- Un ordenador con Windows, macOS o Linux
- Disponer del archivo de instalación de FLECO Studio.

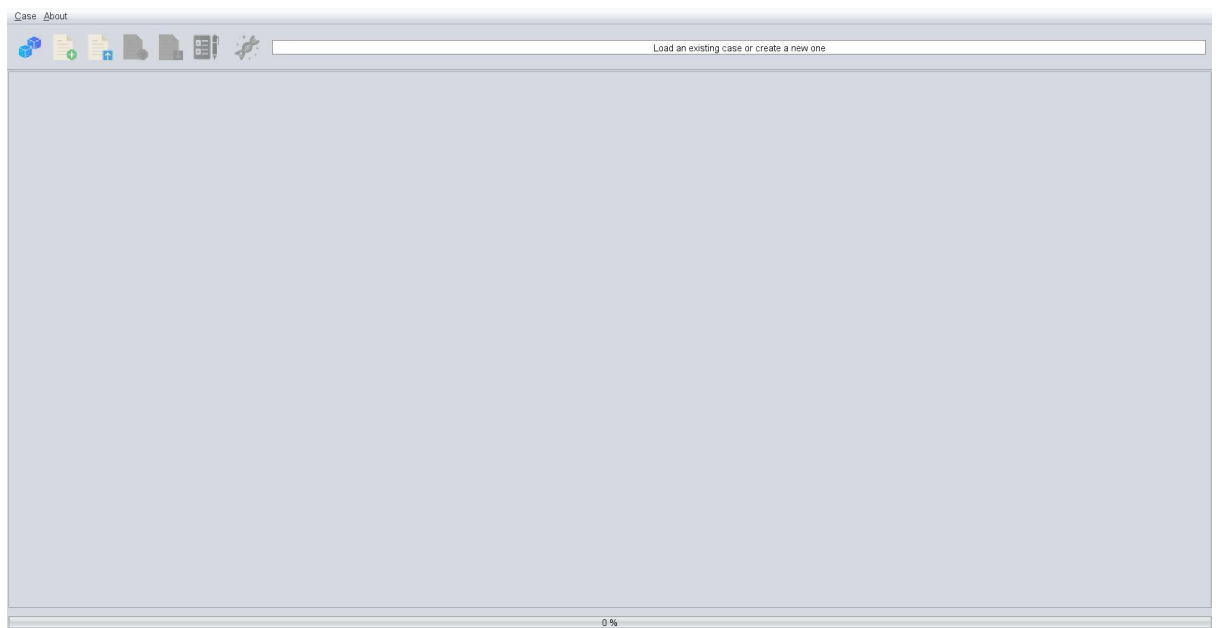
Para instalar FLECO Studio, siga estos pasos:

- Descargue el archivo de instalación de FLECO Studio.
- Ejecute el archivo de instalación.

NAVEGACIÓN

La interfaz de FLECO Studio se divide en dos secciones principales:

- Menú principal: El menú principal le permite acceder a todas las funciones de FLECO Studio.



- Área de trabajo: El área de trabajo es donde se muestran los resultados de los análisis de FLECO Studio.

FLECO Studio - 2_Sesion_2_IC1.fleco					
Case About					
Set the values of current status, constraint operator, and constraint value and run FLECO					
CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Cor
BUSINESS ASSET	---	Several functional areas	0.36702303	GREATER_OR_EQUAL	0.5
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.36500004	N/A	0.0
ID AM	Asset management	Several functional areas	0.41625002	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assessment	0.33	EQUAL	0.3
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	0.0	GREATER_OR_EQUAL	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.0	GREATER_OR_EQUAL	0.0
CSC-3.1	Establish and maintain a data management process	FA5 - Governance	1.0	EQUAL	1.0
CSC-3.2	Establish and maintain a data inventory	FA10 - Security architecture	0.33	EQUAL	0.3
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	1.0	EQUAL	1.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assessment	0.0	GREATER_OR_EQUAL	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.67	EQUAL	0.6
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	GREATER_OR_EQUAL	0.0
ID RA	Risk assessment	Several functional areas	0.33	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assessment	0.33	EQUAL	0.3
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	GREATER_OR_EQUAL	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA8 - Frameworks and standards	0.0	GREATER_OR_EQUAL	0.0
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.47172415	N/A	0.0
PR AC	Identity management, authentication and access control	Several functional areas	0.04714286	N/A	0.0
CSC-4.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	GREATER_OR_EQUAL	0.0
CSC-5.2	Use unique passwords	FA10 - Security architecture	0.0	GREATER_OR_EQUAL	0.0

Antes de poder utilizar FLECO Studio, debe importar los datos de su organización. Los datos que puede importar incluyen:

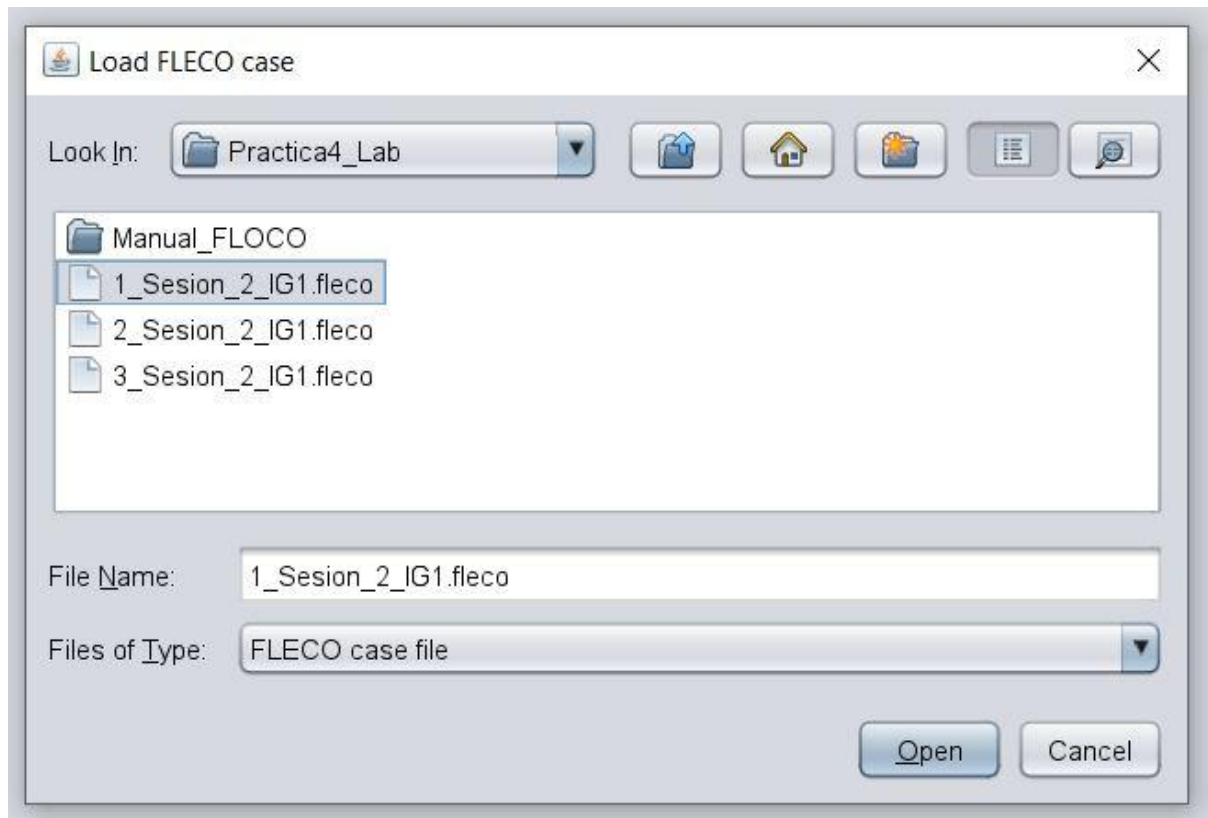
- Información sobre su infraestructura física: Esto puede incluir información sobre sus instalaciones, equipos y personal.
- Información sobre sus sistemas informáticos: Esto puede incluir información sobre sus servidores, redes y aplicaciones.
- Información sobre sus datos: Esto puede incluir información sobre sus bases de datos, archivos y documentos.

Para importar datos en FLECO Studio, siga estos pasos:

- Haga clic en el icono correspondiente:



- Seleccione el archivo a importar y haga clic en "Open".



- Visualizará el archivo importado.

FLECO Studio - 1_Sesion_2_IG1.fleco

Case About

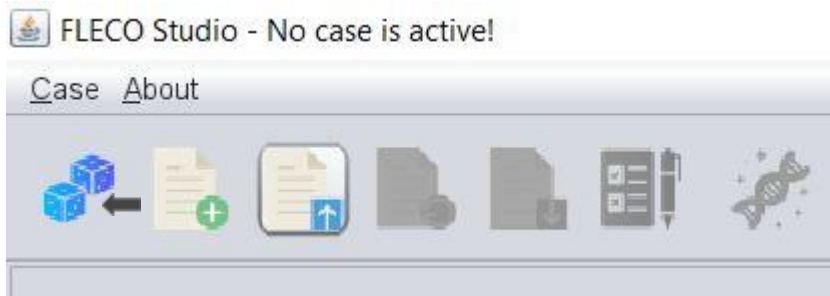
Set the values of current status, constraint operator, and constraint value and run FLECO

CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Cor
BUSINESS ASSET	...	Several functional areas	0.38702303	GREATER_OR_EQUAL	0.5
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.39500004	N/A	0.0
ID-AM	Asset management	Several functional areas	0.41625002	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assessment	0.33	GREATER_OR_EQUAL	0.3
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	0.0	EQUAL	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.0	EQUAL	0.0
CSC-3.1	Establish and maintain a data management process	FA5 - Governance	1.0	GREATER_OR_EQUAL	1.0
CSC-3.2	Establish and maintain a data inventory	FA10 - Security architecture	0.33	GREATER_OR_EQUAL	0.3
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	1.0	GREATER_OR_EQUAL	1.0
ID-AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assessment	0.0	EQUAL	0.0
ID-AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.67	GREATER_OR_EQUAL	0.6
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	EQUAL	0.0
ID-RA	Risk assessment	Several functional areas	0.33	N/A	0.0
ID-RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assessment	0.33	GREATER_OR_EQUAL	0.3
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	EQUAL	0.0
ID-SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA9 - Frameworks and standards	0.0	EQUAL	0.0
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.47172415	N/A	0.0
PR-AC	Identity management, authentication and access control	Several functional areas	0.04714286	N/A	0.0
CSC-4.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	EQUAL	0.0
CSC-5.2	Use unique passwords	FA10 - Security architecture	0.0	EQUAL	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	EQUAL	0.0
PR-AC-3	Remote access is managed	FA10 - Security architecture	0.33	GREATER_OR_EQUAL	0.3
PR-AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	FA10 - Security architecture	0.0	EQUAL	0.0
PR-AC-5	Network integrity is protected	FA10 - Security architecture	0.0	EQUAL	0.0
PR-AC-7	Users, devices, and other assets are authenticated commensurate with the risk of the transaction	FA10 - Security architecture	0.0	EQUAL	0.0
PR-AT	Awareness and training	Several functional areas	1.0	N/A	0.0
PR-AT-1	All users are informed and trained	FA3 - User education	1.0	GREATER_OR_EQUAL	1.0
PR-DS	Data security	Several functional areas	0.83500004	N/A	0.0
CSC-3.4	Enforce data retention	FA10 - Security architecture	0.67	GREATER_OR_EQUAL	0.6
PR-DS-3	Assets are formally managed throughout removal, transfers, and disposition	FA10 - Security architecture	1.0	GREATER_OR_EQUAL	1.0
PR-IP	Information protection processes and procedures	Several functional areas	0.6675	N/A	0.0
ID-9	Depth of defense	FA2 - Security operation	1.0	GREATER_OR_EQUAL	1.0
CSC-11.1	Establish and maintain a data recovery process	FA10 - Security architecture	0.67	GREATER_OR_EQUAL	0.6
CSC-4.3	Configure automatic session locking on enterprise assets	FA10 - Security architecture	1.0	GREATER_OR_EQUAL	1.0
PR-IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA5 - Governance	0.33	GREATER_OR_EQUAL	0.3
PR-IP-11	Cybersecurity is included in human resources practices	FA11 - Career development	0.67	GREATER_OR_EQUAL	0.6
PR-IP-4	Backups of information are conducted, maintained, and tested	FA10 - Security architecture	1.0	GREATER_OR_EQUAL	1.0
PR-IP-6	Data is destroyed according to policy	FA10 - Security architecture	0.67	GREATER_OR_EQUAL	0.6

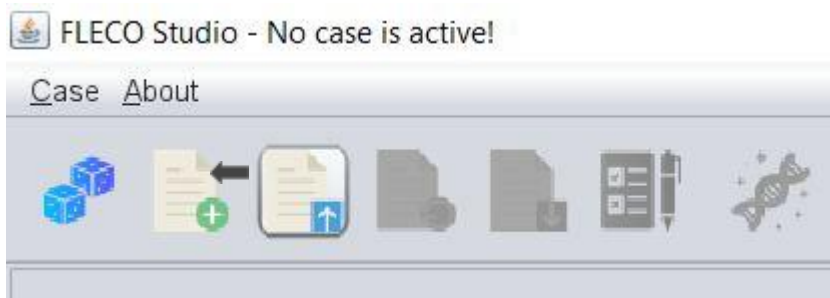
0 %

Para crear un nuevo caso en FLECO Studio, siga estos pasos:

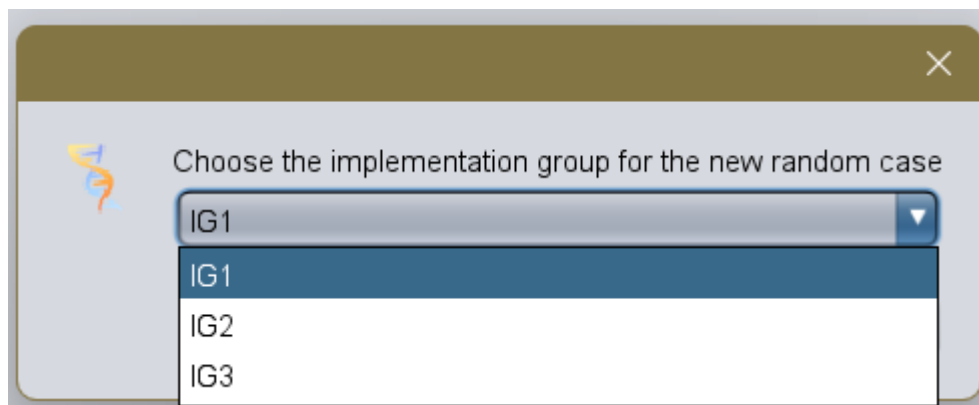
- Existen dos opciones:
 - 1. “New random”: Caso con datos aleatorios, para pruebas.



- 2. “New”: Caso vacío.



.En ambas situaciones, es necesario seleccionar inicialmente el grupo de implementación a aplicar: IG1, IG2 o IG3. Esta elección se realiza en función de la categorización de los activos como de nivel BAJO, MEDIO o ALTO, respectivamente:



Una vez que haya importado los datos de su organización, FLECO Studio puede comenzar a analizar los riesgos de ciberseguridad. FLECO Studio utiliza algoritmos avanzados para evaluar los riesgos de ciberseguridad y generar recomendaciones para mejorar la ciberseguridad de su organización.

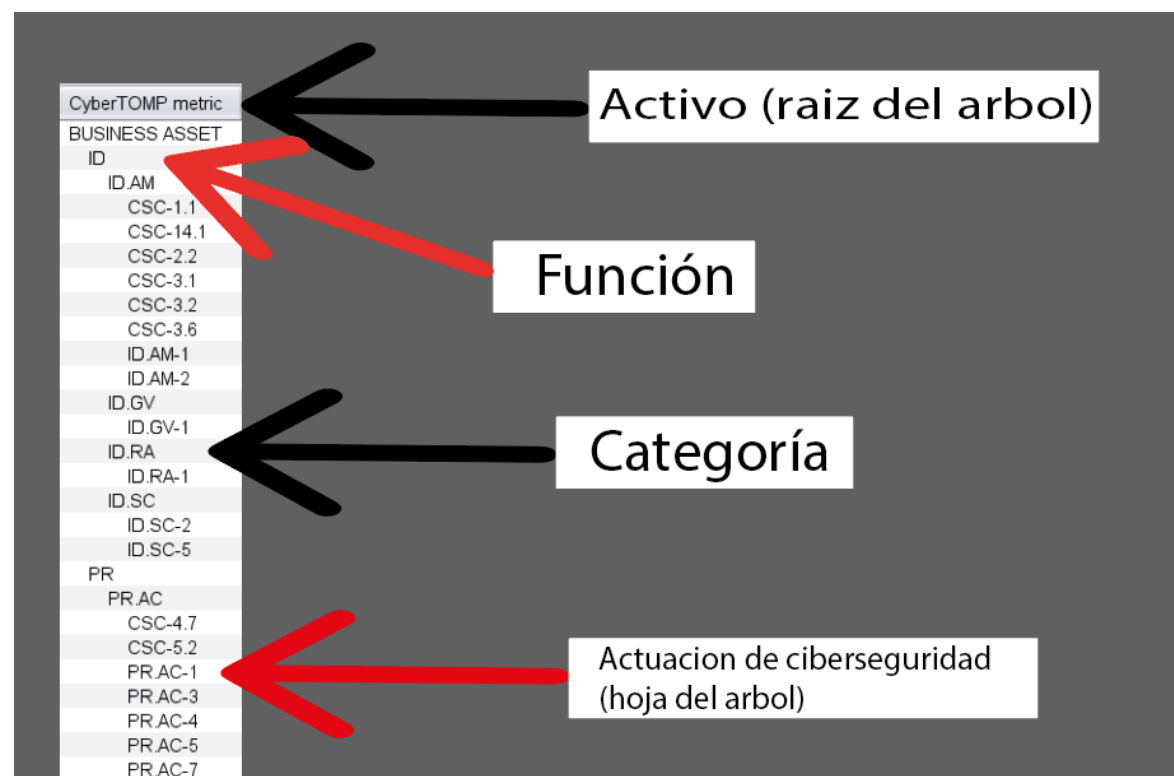
FLECO Studio - 2_Sesion_2_IG1.fleco					
Case About					
Set the values of current status, constraint operator, and constraint value and run FLECO					
CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constra
BUSINESS ASSET	---	Several functional areas	0.38702303	GREATER_OR_EQUAL	0.5
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.30500004	N/A	0.0
ID AM	Asset management	Several functional areas	0.41625002	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assessment	0.33	EQUAL	0.3
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	0.0	GREATER_OR_EQUAL	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.0	GREATER_OR_EQUAL	0.0
CSC-3.1	Establish and maintain a data management process	FA5 - Governance	1.0	EQUAL	1.0
CSC-3.2	Establish and maintain a data inventory	FA10 - Security architecture	0.33	EQUAL	0.3
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	1.0	EQUAL	1.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assessment	0.0	GREATER_OR_EQUAL	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.67	EQUAL	0.6
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	GREATER_OR_EQUAL	0.0
ID RA	Risk assessment	Several functional areas	0.33	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assessment	0.33	EQUAL	0.3
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	GREATER_OR_EQUAL	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA9 - Frameworks and standards	0.0	GREATER_OR_EQUAL	0.0
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.47172415	N/A	0.0
PR AC	Identity management, authentication and access control	Several functional areas	0.04714286	N/A	0.0
CSC-4.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	GREATER_OR_EQUAL	0.0
CSC-5.2	Use unique passwords	FA10 - Security architecture	0.0	GREATER_OR_EQUAL	0.0

Interfaz modo tabla:

CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constra
BUSINESS ASSET	---	Several functional areas	0.38702303	N/A	0.5
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.52833337	N/A	0.0
ID AM	Asset management	Several functional areas	0.58375	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assessment	1.0	N/A	0.0
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	1.0	N/A	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.67	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	0.67	N/A	0.0
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	0.33	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assessment	0.33	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.67	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	1.0	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assessment	1.0	N/A	0.0
ID SC	Supply chain risk management	Several functional areas	0.335	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	0.67	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	0.41344827	N/A	0.0
PR AC	Identity management, authentication and access control	Several functional areas	0.33428574	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	0.67	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	0.67	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	0.33	N/A	0.0
PR AC-7	Users, devices, and other assets are authenticated commensurate with the risk of the transaction	FA10 - Security architecture	0.67	N/A	0.0
PR AT	Awareness and training	Several functional areas	1.0	N/A	0.0
PR AT-1	All users are informed and trained	FA3 - User education	1.0	N/A	0.0
PR DS	Data security	Several functional areas	0.665	N/A	0.0
CSC-3.4	Enforce data retention	FA10 - Security architecture	1.0	N/A	0.0
PR DS-3	Assets are formally managed throughout removal, transfers, and disposition	FA10 - Security architecture	0.33	N/A	0.0
PR IP	Information protection processes and procedures	Several functional areas	0.41625	N/A	0.0
3D-9	Depth of defense	FA2 - Security operation	1.0	N/A	0.0
CSC-11.1	Establish and maintain a data recovery process	FA10 - Security architecture	1.0	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	0.67	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	0.33	N/A	0.0

Vamos a distinguir las distintas columnas que podemos observar:

“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.

Purpose

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Asset management
Establish and maintain detailed enterprise asset inventory
Establish and maintain a security awareness program
Ensure authorized software is currently supported
Establish and maintain a data management process
Establish and maintain a data inventory
Encrypt data on end-user devices
Physical devices and systems within the organization are inventoried
Software platforms and applications within the organization are inventoried
Governance
Organizational cybersecurity policy is established and communicated
Risk assessment
Asset vulnerabilities are identified and documented
Supply chain risk management

“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.

<div>Leading functional area</div> <div>Several functional areas</div> <div>Several functional areas</div> <div>Several functional areas</div> <div>FA7 - Risk assesment</div> <div>FA3 - User education</div> <div>FA8 - Application security</div> <div>FA5 - Governance</div> <div>FA10 - Security architecture</div> <div>FA10 - Security architecture</div>
<p>“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:</p> <ul style="list-style-type: none"> • 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.
<div>Current status</div> <div>0.38702303</div> <div>0.30500004</div> <div>0.41625002</div> <div>0.33</div> <div>0.0</div> <div>0.0</div> <div>1.0</div> <div>0.33</div> <div>1.0</div>
<p>“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).</p>

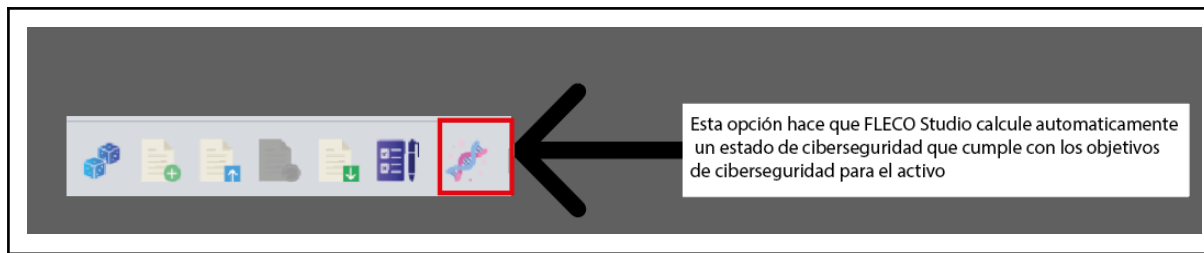
<div>Constraint operator</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div> <div>N/A</div>
<div>“Constraint value”: Permite definir el valor específico asociado al operador.</div>
<div>Constra</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div> <div>0.0</div>
<div>“Target status”: En esta columna FLECO Studio sugiere valores específicos de implementación de cada actuación de ciberseguridad que cumplen con los objetivos estratégicos definidos. Sólo para el modo “Automático/Guiado”.</div>



Una vez que haya importado los datos de su organización, FLECO Studio puede comenzar a analizar los riesgos de ciberseguridad. FLECO Studio utiliza algoritmos avanzados para evaluar los riesgos de ciberseguridad y generar recomendaciones para mejorar la ciberseguridad de su organización.

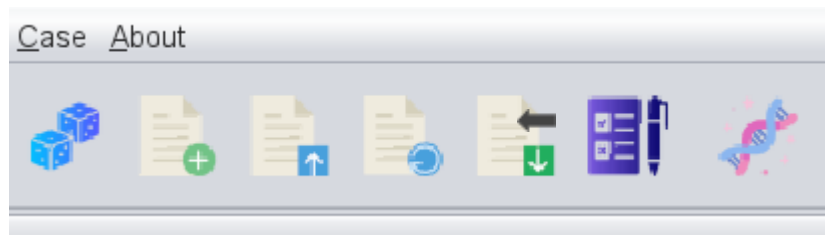
Hay dos formas de trabajar:

- 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: 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:

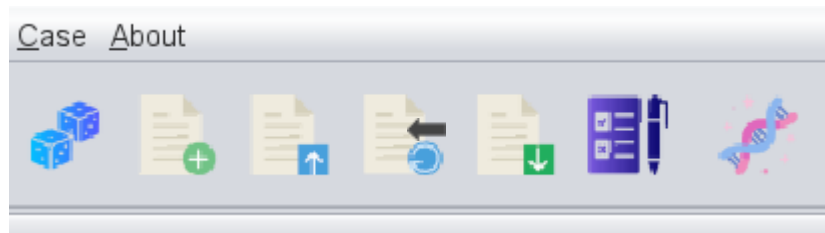


Por ultimo, el caso se puede guardar o cargar de disco guardar el caso existen dos opciones:

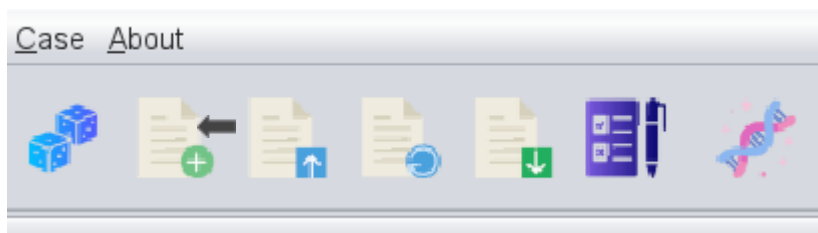
- 1.A la hora de guardar existen dos opciones:
 - Guardar con un otro nombre:



- Guardar con el mismo nombre:



- 2.Cargar de disco.



CONCLUSIÓN

FLECO Studio es una herramienta poderosa que puede ayudar a las organizaciones a implementar una ciberseguridad holística. Este manual de usuario le ayudará a familiarizarse con FLECO Studio y a comenzar a utilizarlo para mejorar la ciberseguridad de su organización.

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

La Licencia Pública General Menor de GNU (LGPL), gestada por la Free Software Foundation, se presenta como un marco para el software libre con un enfoque singular en bibliotecas y componentes reutilizables. Su distintivo radica en la capacidad de permitir la vinculación con software propietario sin imponer la condición de convertirlo en software libre. Esto la distingue de manera significativa de la Licencia Pública General de GNU, otorgando una flexibilidad destacada en términos de uso y distribución de estos elementos.

La licencia de FLECO Studio ofrece una serie de características principales que la convierten en una herramienta ideal para la creación de aplicaciones de e-learning. Estas características incluyen:

- **Soporte para múltiples idiomas:** FLECO Studio permite crear aplicaciones de e-learning en múltiples idiomas, lo que lo hace ideal para empresas y organizaciones que operan a nivel internacional.
- **Personalización:** FLECO Studio ofrece una gran cantidad de opciones de personalización, lo que permite a los desarrolladores crear aplicaciones de e-learning que se adapten a las necesidades específicas de sus usuarios.
- **Facilidad de uso:** FLECO Studio es una herramienta fácil de usar, incluso para los desarrolladores sin experiencia en e-learning.

3. Licencia el manual de usuario, seleccionando la licencia Creative Commons adecuada:

Este trabajo tiene licencia CC BY-NC-SA 4.0.

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

La licencia Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) es una licencia de derechos de autor que permite a los usuarios copiar, distribuir, exhibir, y realizar obras derivadas del trabajo original, siempre que se atribuya a los autores originales, no se utilice para fines comerciales y se publique bajo la misma licencia.

Esta licencia es adecuada para el manual de usuario de FLECO Studio porque permite a los usuarios compartir y reutilizar el contenido del manual de forma libre y abierta, con algunas restricciones. La atribución a los autores originales ayuda a garantizar que se reconozca su trabajo. La prohibición de utilizar el contenido para fines comerciales ayuda a proteger los derechos de los autores y a garantizar que el manual se utilice de forma adecuada. La condición de compartir bajo la misma licencia ayuda a garantizar que el contenido del manual de usuario de FLECO Studio se mantenga disponible de forma libre y abierta.

Las principales características de la licencia CC BY-NC-SA 4.0 son las siguientes:

Atribución: Los usuarios deben atribuir el trabajo original a los autores originales. Esto se puede hacer de cualquier manera razonable, pero debe incluir el nombre de los autores, el título del trabajo y el enlace a la licencia.

No comercial: Los usuarios no pueden utilizar el trabajo para fines comerciales. Esto significa que los usuarios no pueden vender o comercializar el trabajo, ni utilizarlo para promocionar sus productos o servicios.

Compartir bajo la misma licencia: Los usuarios pueden redistribuir o crear obras derivadas del trabajo, pero deben hacerlo bajo la misma licencia CC BY-NC-SA 4.0.

En conclusión, la licencia CC BY-NC-SA 4.0 es adecuada para el manual de usuario de FLECO Studio porque permite a los usuarios compartir y reutilizar el contenido del manual de forma libre y abierta, con algunas restricciones.

SESIÓN 2

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.

Para este ejercicio, he tomado los siguientes activos de negocio imaginarios:

- Activo 1: Base de datos de clientes de una pequeña empresa.
- Activo 2: Sistema de control industrial de una fábrica.
- Activo 3: Red interna de una empresa multinacional.

He clasificado estos activos de la siguiente manera:

- Activo 1: Criticidad baja
- Activo 2: Criticidad media
- Activo 3: Criticidad alta

He utilizado FLECO Studio para crear estos tres casos, vacíos, y contar los valores preguntados, que se encuentran en la primera columna de la aplicación. Los resultados son los siguientes:

ACTIVO	FUNCIONES DE CIBERSEGURIDAD	CATEGORÍAS DE CIBERSEGURIDAD	ACTUACIONES DE CIBERSEGURIDAD
G1	4	15	47
G2	4	20	107
G3	5	23	167

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

Relación entre el número de funciones, categorías y resultados esperados y el nivel de criticidad del activo

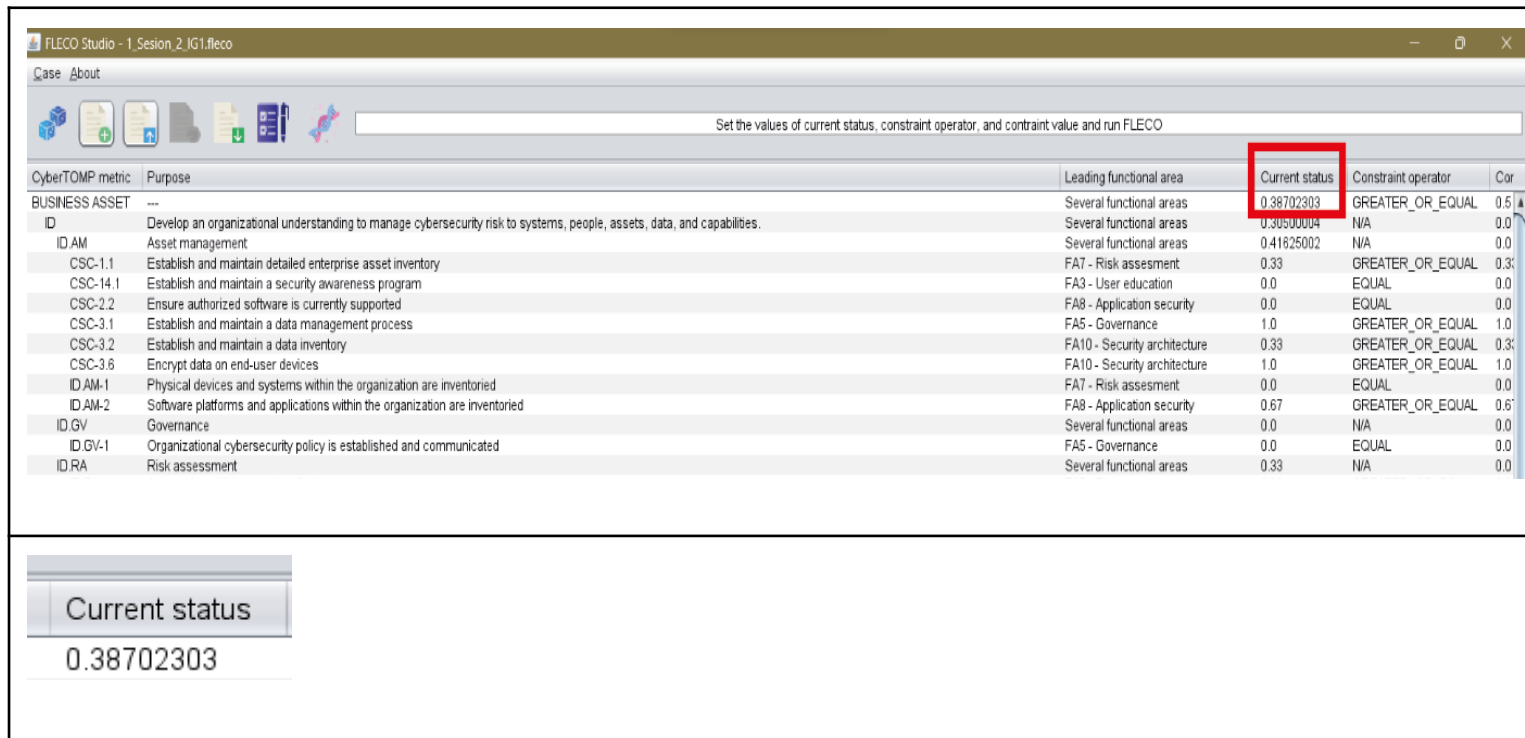
Los datos obtenidos muestran que, en general, el número de funciones, categorías y resultados esperados aumenta en proporción al nivel de criticidad del activo. Esto se debe a que los activos de mayor criticidad son los más susceptibles de sufrir un incidente cibernético con un impacto significativo. Por lo tanto, requieren una mayor protección.

Esta relación es coherente con el principio de proporcionalidad en la aplicación de la ciberseguridad, el cual establece que la ciberseguridad de un activo debe abordarse en proporción a la criticidad y el impacto de un posible incidente cibernético.

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.



FLECO Studio - 1_Sesion_2_IG1.fleco

Case About

Set the values of current status, constraint operator, and constraint value and run FLECO

CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Cor
BUSINESS ASSET	---	Several functional areas	0.38702303	GREATER_OR_EQUAL	0.5
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.30500004	N/A	0.0
ID AM	Asset management	Several functional areas	0.41625002	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	FA7 - Risk assessment	0.33	GREATER_OR_EQUAL	0.33
CSC-14.1	Establish and maintain a security awareness program	FA3 - User education	0.0	EQUAL	0.0
CSC-2.2	Ensure authorized software is currently supported	FA8 - Application security	0.0	EQUAL	0.0
CSC-3.1	Establish and maintain a data management process	FA5 - Governance	1.0	GREATER_OR_EQUAL	1.0
CSC-3.2	Establish and maintain a data inventory	FA10 - Security architecture	0.33	GREATER_OR_EQUAL	0.33
CSC-3.6	Encrypt data on end-user devices	FA10 - Security architecture	1.0	GREATER_OR_EQUAL	1.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA7 - Risk assessment	0.0	EQUAL	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA8 - Application security	0.67	GREATER_OR_EQUAL	0.67
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	EQUAL	0.0
ID RA	Risk assessment	Several functional areas	0.33	N/A	0.0

Current status

0.38702303

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.

Modificamos ciertos valores de la columna “Current status” para lograr el valor deseado de al menos 0,5 en el nivel global de ciberseguridad del activo:

Current status
0.5014541

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?

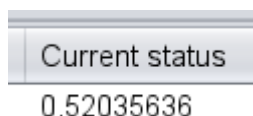
Sí, he identificado algunas formas de mejorar la ciberseguridad de un activo modificando algunos valores de la columna “*Current status*”, es decir, aumentar el número de sub actuaciones de una actividad/actuación de ciberseguridad. En concreto se han incrementado los recursos de áreas como “*Security Architecture*”, “*Application Security*”, “*Risk Assessment*”. Por otro lado el incremento de estas áreas pueden implicar un esfuerzo adicional para otras áreas que no estaban aportando a la ciberseguridad y aumentar el esfuerzo de áreas que ya estaban aportando a la ciberseguridad del activo.

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.

Modificamos ciertos valores de la columna “*Current status*” para lograr el valor deseado de al menos 0,5 en el nivel global de ciberseguridad del activo:



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?

Si, para mejorar la ciberseguridad del activo hemos aumentado el número de sub actuaciones de actividades que no estaban implementadas. “*User education*”, “*Risk Assessment*” y “*Governance*” han sido algunas áreas que se han incrementado. Este incremento puede implicar un esfuerzo adicional para otras áreas que no estaban aportando a la ciberseguridad y aumentar el esfuerzo de áreas que ya estaban aportando a la ciberseguridad del activo.

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 recatalogado con una criticidad mayor por algún motivo. Ahora, réplica 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.

-Valor del nivel global de ciberseguridad del activo de “3_Sesion_2_IG1.fleco” :0.38702303
-Valor del nivel global de ciberseguridad del activo creado “3_Sesion_2_IG1_manual.fleco”:
0.08174858

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?

Sí, se puede argumentar que hay un efecto sobre el nivel de ciberseguridad global del activo en relación con su cambio de criticidad. El nivel de ciberseguridad global del activo creado nos da un valor menor al del primero ya que con las actuaciones implementadas del activo con menor criticidad no basta para llegar al mismo valor que teníamos en este activo debido a que aumenta su criticidad.

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 lograr un valor exacto, pero uno aproximado sirve para lo que se pretende en este ejercicio. Guarda los cambios cuando lo hayas logrado.

Current status
0.38722682

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?

Para lograr un nivel de ciberseguridad similar hemos incrementado el número de subactuaciones de ciertas actividades que o bien no estaban aportando nada o bien podían aportar algo más.

SESIÓN 3

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?

Activo 1: Crítico Bajo

FA2 - Security operation: 5 ocasiones
FA3 - User education: 2 ocasiones
FA5 - Governance: 12 ocasiones
FA7 - Risk assessment: 4 ocasiones
FA8 - Application security: 2 ocasiones
FA9 - Frameworks and standards: 1 ocasión
FA10 - Security architecture: 22 ocasiones
FA11 - Career development: 1 ocasión

Activo 2: Crítico Medio

FA2 - Security operation: 14 ocasiones
FA3 - User education: 5 ocasiones
FA5 - Governance: 35 ocasiones

FA7 - Risk assessment: 12 ocasiones
FA8 - Application security: 6 ocasiones
FA9 - Frameworks and standards: 6 ocasiones
FA10 - Security architecture: 53 ocasiones
FA11 - Career development: 1 ocasión

Activo 3: Crítico Alto

FA1 - Physical security: 1 ocasión
FA2 - Security operation: 55 ocasiones
FA3 - User education: 4 ocasiones
FA4 - Threat intelligence: 4 ocasiones
FA5 - Governance: 47 ocasiones
FA6 - Enterprise risk management: 16 ocasiones
FA7 - Risk assessment: 16 ocasiones
FA8 - Application security: 6 ocasiones
FA9 - Frameworks and standards: 13 ocasiones
FA10 - Security architecture: 57 ocasiones
FA11 - Career development: 3 ocasiones
FA12 - Communication and relationships: 3 ocasiones

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?

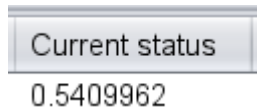
- El activo de criticidad baja cuenta con un total de 9 áreas funcionales distintas, con un promedio de 5,6 ocasiones por área funcional.
- El activo de criticidad media cuenta con un total de 12 áreas funcionales distintas, con un promedio de 11,6 ocasiones por área funcional.
- El activo de criticidad alta cuenta con un total de 18 áreas funcionales distintas, con un promedio de 3,1 ocasiones por área funcional.

Esta relación se observa también en el número de veces que cada área funcional podría contribuir a la ciberseguridad del activo. En general, las áreas funcionales que más veces aparecen son las relacionadas con la seguridad operativa, como FA2 - Security operation y FA3 - User education. Estas áreas funcionales son esenciales para la detección y respuesta a los incidentes de ciberseguridad, independientemente del nivel de criticidad del activo.

La relación observada entre el nivel de criticidad del activo y el número de áreas funcionales distintas y el número de veces que cada una de ellas podría contribuir a la ciberseguridad es razonable. Los activos de mayor criticidad requieren un mayor esfuerzo de seguridad, que debe incluir un enfoque holístico que abarque un mayor número de áreas funcionales.

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.*

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?

Para mejorar la ciberseguridad del activo hemos mejorado o implementado todas las actuaciones respetando las restricciones de las columnas Constraint operator + Constraints value. Para las actuaciones que ya estaban aportando a la ciberseguridad ahora lo harán más y también contribuirán a la ciberseguridad del activo las actuaciones que hasta ahora no lo estaban haciendo.

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.

Current status
0.5409962

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?

No hemos conseguido el nivel de ciberseguridad deseado ya que al incrementar el número de subactuaciones de las actividades que ya estaban participando no es suficiente para conseguir el valor de al menos 0,6 en la ciberseguridad del activo.

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.

Current status
0.6097203

b) A la vista de lo realizado en el ejercicio ¿has conseguido el objetivo global de ciberseguridad del activo? ¿Qué diferencia tiene 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?

Sí, se ha conseguido el objetivo global de ciberseguridad del activo, que era de al menos 0,6. La principal diferencia con el caso del ejercicio anterior es que en este caso se han implementado subactuaciones de actividades que no estaban contribuyendo a la ciberseguridad del activo. En este caso se ha mejorado o implementado la participación en la ciberseguridad del activo de todas las actuaciones hasta llegar al nivel de ciberseguridad requerido, desequilibrando así la participación de cada área ya que solo se han mejorado o implementado la participación de áreas hasta llegar al nivel deseado y las otras no se han modificado. La decisión de que posible combinación de áreas/actuaciones se implementa le corresponde a la empresa.

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.

Current status
1.0

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?

Si es posible conseguir un valor global de ciberseguridad del activo de 1,0 aumentando o implementando la participación de todas las actuaciones al máximo para garantizar la totalidad del nivel buscado. Esta es la única manera de conseguir este nivel de ciberseguridad del activo.

SESIÓN 4

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 funciones de ciberseguridad podrían potencialmente contribuir a la ciberseguridad para cada uno de los activos? Y para cada una de ellas ¿Cuántas categorías distintas? 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. No es necesario guardar los casos.

Tabla que contiene el número de funciones por cada categoría de criticidad

	FUNCIONES
IG1	4
IG2	4
IG3	5

Tabla que contiene el número de subfunciones por función según el grado de criticidad

FUNCIONES	IG1	IG2	IG3
ID	4	6	6
PR	6	6	6
DE	3	3	3
RS	2	5	5
RC	-	-	3

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

A medida que la criticidad de un activo de negocio aumenta, se requieren más funciones de ciberseguridad distribuidas en diferentes categorías para protegerlo adecuadamente. Esta relación parece lógica, ya que los activos más críticos necesitan una mayor atención y medidas de seguridad para mitigar posibles amenazas. La distribución de funciones y categorías refleja la importancia asignada a cada aspecto de la ciberseguridad en función del nivel de criticidad del activo.

Ejercicio 2. A continuación, abre el caso 1_Sesion_4_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 0,29974717. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, deben seguir sin aplicarse. En este caso son las funciones de ciberseguridad Identificar (ID) y Detectar (DE), así como todas las categorías y actuaciones de ciberseguridad derivadas.

- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar. Es decir, que tengan una mayor contribución a la ciberseguridad del activo aprovechando que ya están aplicándose.

- El nivel global buscado, de ciberseguridad del activo, 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_4_IG1_manual.fleco.

Current status
0.50574714

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?

Sí, se ha conseguido el objetivo global de ciberseguridad del activo de al menos 0,5. Para ello se ha incrementado la profundidad de las actuaciones de ciberseguridad que ya estaban participando y de algunas que no lo estaban haciendo menos las actuaciones de las funciones de ciberseguridad Identificar (ID) y Detectar (DE) como nos indica el enunciado.

Ejercicio 3. A continuación, abre el caso 2_Sesion_4_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 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, deben seguir sin aplicarse. En este caso son las funciones de ciberseguridad “Identificar” (ID) y “Detectar” (DE), así como todas las categorías y actuaciones de ciberseguridad derivadas.

- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar. Es decir, que tengan una mayor contribución a la ciberseguridad del activo aprovechando que ya están aplicándose.

- 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 tengas hecha una u otra cosa, guárdalo como 2_Sesion_4_IG1_manual.fleco.

Current status
0.53333336

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?

En este caso no se ha conseguido el nivel global buscado de ciberseguridad de al menos 0,6 ya que incrementando la participación de las actuaciones que ya estaban participando y de

algunas que no estaban no es suficiente. Para obtener un mejor resultado habría que haber incrementado la participación de actuaciones que el enunciado nos indica de no implementar.

Ejercicio 4. A continuación, abre el caso 3_Sesion_4_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 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene una serie de objetivos/restricciones estratégicas de ciberseguridad definidas, consistentes básicamente en:

- Aquellas dimensiones de la ciberseguridad que todavía no se están aplicando a la ciberseguridad del activo, pueden comenzar a aplicarse.
- Aquellas dimensiones de la ciberseguridad que ya se estén aplicando a la ciberseguridad del activo, pueden seguir aplicándose, implementándose con mayor profundidad las actuaciones de ciberseguridad parcialmente implementadas o implementando aquellas que aún no se han empezado a implementar. - 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_4_IG1_manual.fleco.

Current status
0.60324144

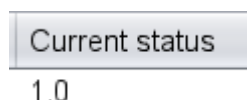
b) A la vista de lo realizado en el ejercicio ¿has conseguido el objetivo global de ciberseguridad del activo? ¿Qué diferencia tiene este caso del descrito en el ejercicio anterior? ¿Qué implicaciones tiene sobre las dimensiones aplicadas al activo? ¿Están más o menos equilibradas?

En este caso no se ha conseguido el nivel global buscado de ciberseguridad de al menos 0,6 ya que incrementando la participación de las actuaciones que ya estaban participando y de algunas que no estaban no es suficiente. Con respecto al ejercicio anterior hemos podido implementar o mejorar la participación de cualquier actuación sin restricciones. Las dimensiones que hemos implementado o mejorado tendrán más implicación en la ciberseguridad del caso y estarán menos equilibradas ya que las que hemos modificado lo hemos hecho al máximo hasta obtener el nivel de ciberseguridad requerido y los demás los hemos dejado como estaban.

Ejercicio 5. A continuación, abre el caso 4_Sesion_4_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 0,29974717. Es el mismo caso del ejercicio anterior. Verás que tiene un único objetivo/restricción estratégica de ciberseguridad definida, consistente básicamente en:

- El nivel global de ciberseguridad del activo buscado es exactamente 1.0, 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_4_IG1_manual.fleco.



Current status
1.0

b) A la vista de lo realizado en el 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?

Si es posible conseguir un valor global de ciberseguridad del activo de 1,0 aumentando o implementando la participación de todas las actuaciones al máximo para garantizar la totalidad del nivel buscado. Esta es la única manera de conseguir este nivel de ciberseguridad del activo.

SESIÓN 5

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 – Communication 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.

Current status
0.40924883

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.

FA12 - Communication and relationships	0.0	LESS	1.0	0.0
FA12 - Communication and relationships	0.67	EQUAL	1.0	1.0
FA12 - Communication and relationships	0.33	EQUAL	1.0	1.0

Hemos diseñado restricciones en el área citada para mantener los valores de ciberseguridad al nivel original.

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?

Target status
0.4164952

Una vez calculada la solución por fleco se han cambiado algunos valores de la columna Target status que se muestran en rojo en la siguiente imagen:

Several functional areas	0.05555556	N/A	0.0	0.11111112
Several functional areas	0.33333334	N/A	0.0	0.6666667
FA12 - Communication and relationships	0.0	LESS	1.0	0.0
FA12 - Communication and relationships	0.67	EQUAL	1.0	1.0
FA12 - Communication and relationships	0.33	EQUAL	1.0	1.0

Así como el valor total:

Target status
0.4164952

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?

Para que nuestra ciberseguridad siga siendo efectiva, tenemos que estar siempre adaptándonos y revisando nuestras estrategias. Es como estar siempre un paso adelante, porque las amenazas que enfrentamos no dejan de cambiar. El área funcional que ha asumido el coste de estos ajustes es la FA12 – Communication and relationships

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.

Modificaciones realizadas para el área FA7 – Risk assessment:

→Para cada entrada de dicha área realizamos los siguientes cambios:

- Cambiar el "Constraint operator" a "equal" .
- Establecer el "Constraint value" a 0.0 .

Modificaciones realizadas para el área *F09- Framework and standards*:

→Para cada entrada de dicha área realizamos los siguientes cambios:

- Cambiar el "Constraint operator" a "equal" .
- Establecer el "Constraint value" al mismo que "Current status".

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

Modificaciones para el global del activo del negocio:

- Cambiar el "Constraint operator" a "greater or equal".
- Establecer el "Constraint value" a *0,4164952* .

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?



Una vez se ha calculado la solución de forma automática por Fleco se puede observar cómo se han modificado valores de otras áreas a FA7 y F09 para compensar su limitación a la contribución a la ciberseguridad del activo.

d) Guarda el caso como 2_Sesion_5_IG3_manual_automatico.fleco.

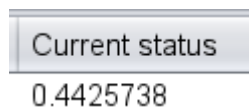
e) A la vista de lo realizado en este ejercicio, ¿Has entendido que por necesidades del negocio puede ser necesario que la participación de ciertas áreas en la ciberseguridad del activo se vea limitada? ¿En este caso, si tuvieras que resumir en una frase qué ha habido que hacer para mantener el nivel 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?

Este ejemplo nos muestra que, a veces, las demandas del negocio pueden llevar a que tengamos que cambiar cómo ciertas áreas contribuyen a la ciberseguridad del activo. El área funcional que ha asumido el coste de estos ajustes son todas menos las áreas limitadas FA7 y F09.

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?

La tarea realizada muestra claramente que cuando una empresa decide cambiar la categoría de importancia de uno de sus activos, también tiene que ajustar las acciones de protección cibernética correspondientes. Esto varía si el nivel de riesgo asignado aumenta o disminuye. En esta ocasión, a pesar de que el activo ha pasado a una categoría de menor importancia, el nivel de ciberseguridad se ha preservado o incluso reforzado. Esto indica una gestión de seguridad muy eficiente. Cuando ciertas métricas ya no son relevantes para el activo debido a este cambio, significa que las áreas que antes se enfocaban en esas medidas específicas ahora pueden necesitar reenfocar sus esfuerzos o incluso discontinuar ciertas prácticas. Las estrategias de ciberseguridad que ya no son necesarias se ajustan, liberando recursos y permitiendo que la organización se concentre en las áreas de mayor prioridad.

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.

Target status
0.49491307

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?

Si, es posible mantener o incluso mejorar el nivel de ciberseguridad de un activo involucrando a múltiples áreas funcionales en lugar de depender de una sola, lo cual puede ayudar a evitar su saturación. La participación de diferentes áreas permite una distribución más equitativa de la carga de trabajo. Sin embargo no hubiese sido posible lograr el nivel de ciberseguridad requerido solo utilizando el área funcional original ya que al principio todas las entradas de este área estaban implementadas al máximo y no se llegaba al nivel requerido. La opción más holística y potencialmente más beneficiosa para la organización es aquella en la que participan todas las áreas relevantes. Esta estrategia no solo distribuye la carga de trabajo, sino que también asegura una visión más amplia y completa de la ciberseguridad