

Manual de Fleco Studio



Realizado por Guadalupe Gómez 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 aglutan 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

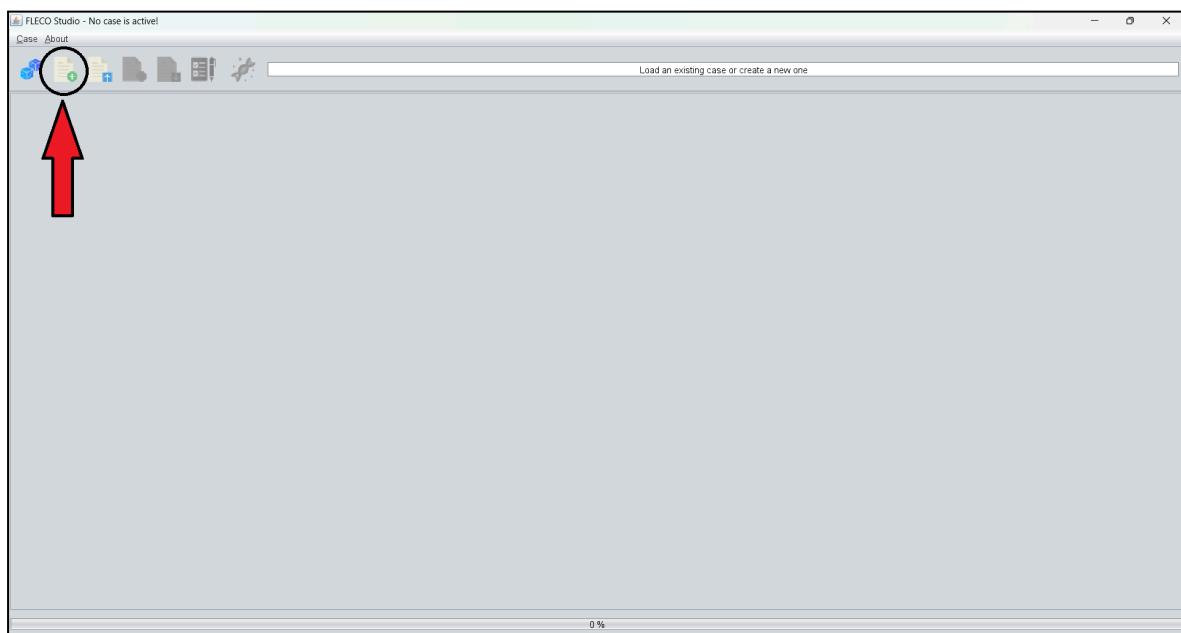


Figura 2. Creación de un nuevo caso vacío

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

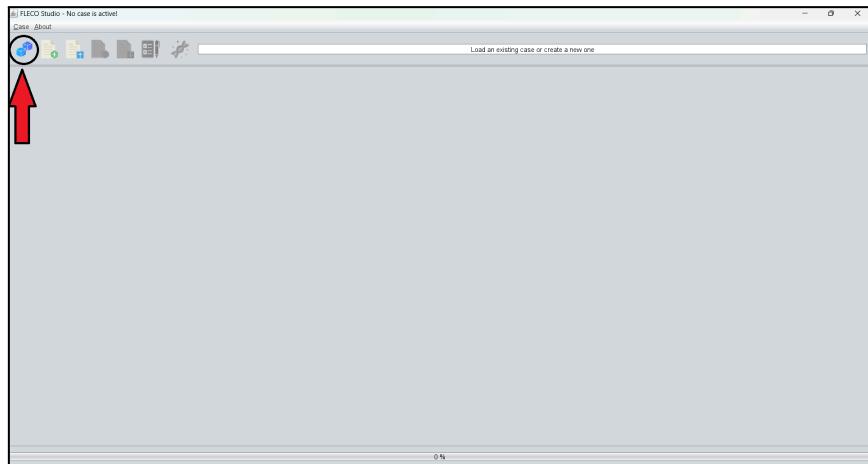


Figura 4. Creación de un caso aleatorio

Esta opción nos permite crear un nuevo caso que, al contrario que la opción anterior, se nos llenará 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:

The screenshot shows the FIECO Studio application window. At the top, there's a menu bar with 'File', 'Edit', 'Case', 'About'. Below the menu is a toolbar with icons for file operations like Open, Save, Print, etc. The main area is titled 'CyberTOMP metric: Purpose' and contains a table with data. The table has columns for 'Leading functional area', 'Current status', 'Constraint operator', and 'Constra...'. The data is organized into sections: BUSINESS ASSET, CSC-1, CSC-2, CSC-3, CSC-4, CSC-5, PR-AC, PR-DS, PR-P, and PR-R. Each section contains several rows of data, such as 'Establish an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities' under CSC-1.

Set the values of current status, constraint operator, and constraint value and run FIECO			
	Leading functional area	Current status	Constraint operator
CSC-1.1	Several functional areas	0.0	N/A
CSC-1.2	Several functional areas	0.0	N/A
CSC-1.3	Several functional areas	0.0	N/A
CSC-1.4	FAT - Risk assessment	0.0	N/A
CSC-1.5	FAT - User education	0.0	N/A
CSC-1.6	FAT - Physical security	0.0	N/A
CSC-1.7	FAT - Governance	0.0	N/A
CSC-1.8	FAT - Security architecture	0.0	N/A
CSC-1.9	FAT - Security operation	0.0	N/A
CSC-1.10	Several functional areas	0.0	N/A
CSC-1.11	FAT - Risk assessment	0.0	N/A
CSC-1.12	FAT - Physical security	0.0	N/A
CSC-1.13	FAT - Governance	0.0	N/A
CSC-1.14	FAT - Security architecture	0.0	N/A
CSC-1.15	FAT - Security operation	0.0	N/A
CSC-1.16	Several functional areas	0.0	N/A
CSC-1.17	FAT - Risk assessment	0.0	N/A
CSC-1.18	FAT - Physical security	0.0	N/A
CSC-1.19	FAT - Governance	0.0	N/A
CSC-1.20	FAT - Security architecture	0.0	N/A
CSC-1.21	FAT - Security operation	0.0	N/A
CSC-1.22	Several functional areas	0.0	N/A
CSC-1.23	FAT - Risk assessment	0.0	N/A
CSC-1.24	FAT - Physical security	0.0	N/A
CSC-1.25	FAT - Governance	0.0	N/A
CSC-1.26	FAT - Security architecture	0.0	N/A
CSC-1.27	FAT - Security operation	0.0	N/A
CSC-1.28	Several functional areas	0.0	N/A
CSC-1.29	FAT - Risk assessment	0.0	N/A
CSC-1.30	FAT - Physical security	0.0	N/A
CSC-1.31	FAT - Governance	0.0	N/A
CSC-1.32	FAT - Security architecture	0.0	N/A
CSC-1.33	FAT - Security operation	0.0	N/A
CSC-1.34	Several functional areas	0.0	N/A
CSC-1.35	FAT - Risk assessment	0.0	N/A
CSC-1.36	FAT - Physical security	0.0	N/A
CSC-1.37	FAT - Governance	0.0	N/A
CSC-1.38	FAT - Security architecture	0.0	N/A
CSC-1.39	FAT - Security operation	0.0	N/A
CSC-1.40	Several functional areas	0.0	N/A
CSC-1.41	FAT - Risk assessment	0.0	N/A
CSC-1.42	FAT - Physical security	0.0	N/A
CSC-1.43	FAT - Governance	0.0	N/A
CSC-1.44	FAT - Security architecture	0.0	N/A
CSC-1.45	FAT - Security operation	0.0	N/A
CSC-1.46	Several functional areas	0.0	N/A
CSC-1.47	FAT - Risk assessment	0.0	N/A
CSC-1.48	FAT - Physical security	0.0	N/A
CSC-1.49	FAT - Governance	0.0	N/A
CSC-1.50	FAT - Security architecture	0.0	N/A
CSC-1.51	FAT - Security operation	0.0	N/A
CSC-1.52	Several functional areas	0.0	N/A
CSC-1.53	FAT - Risk assessment	0.0	N/A
CSC-1.54	FAT - Physical security	0.0	N/A
CSC-1.55	FAT - Governance	0.0	N/A
CSC-1.56	FAT - Security architecture	0.0	N/A
CSC-1.57	FAT - Security operation	0.0	N/A
CSC-1.58	Several functional areas	0.0	N/A
CSC-1.59	FAT - Risk assessment	0.0	N/A
CSC-1.60	FAT - Physical security	0.0	N/A
CSC-1.61	FAT - Governance	0.0	N/A
CSC-1.62	FAT - Security architecture	0.0	N/A
CSC-1.63	FAT - Security operation	0.0	N/A
CSC-1.64	Several functional areas	0.0	N/A
CSC-1.65	FAT - Risk assessment	0.0	N/A
CSC-1.66	FAT - Physical security	0.0	N/A
CSC-1.67	FAT - Governance	0.0	N/A
CSC-1.68	FAT - Security architecture	0.0	N/A
CSC-1.69	FAT - Security operation	0.0	N/A
CSC-1.70	Several functional areas	0.0	N/A
CSC-1.71	FAT - Risk assessment	0.0	N/A
CSC-1.72	FAT - Physical security	0.0	N/A
CSC-1.73	FAT - Governance	0.0	N/A
CSC-1.74	FAT - Security architecture	0.0	N/A
CSC-1.75	FAT - Security operation	0.0	N/A
CSC-1.76	Several functional areas	0.0	N/A
CSC-1.77	FAT - Risk assessment	0.0	N/A
CSC-1.78	FAT - Physical security	0.0	N/A
CSC-1.79	FAT - Governance	0.0	N/A
CSC-1.80	FAT - Security architecture	0.0	N/A
CSC-1.81	FAT - Security operation	0.0	N/A
CSC-1.82	Several functional areas	0.0	N/A
CSC-1.83	FAT - Risk assessment	0.0	N/A
CSC-1.84	FAT - Physical security	0.0	N/A
CSC-1.85	FAT - Governance	0.0	N/A
CSC-1.86	FAT - Security architecture	0.0	N/A
CSC-1.87	FAT - Security operation	0.0	N/A
CSC-1.88	Several functional areas	0.0	N/A
CSC-1.89	FAT - Risk assessment	0.0	N/A
CSC-1.90	FAT - Physical security	0.0	N/A
CSC-1.91	FAT - Governance	0.0	N/A
CSC-1.92	FAT - Security architecture	0.0	N/A
CSC-1.93	FAT - Security operation	0.0	N/A
CSC-1.94	Several functional areas	0.0	N/A
CSC-1.95	FAT - Risk assessment	0.0	N/A
CSC-1.96	FAT - Physical security	0.0	N/A
CSC-1.97	FAT - Governance	0.0	N/A
CSC-1.98	FAT - Security architecture	0.0	N/A
CSC-1.99	FAT - Security operation	0.0	N/A
CSC-1.100	Several functional areas	0.0	N/A
CSC-1.101	FAT - Risk assessment	0.0	N/A
CSC-1.102	FAT - Physical security	0.0	N/A
CSC-1.103	FAT - Governance	0.0	N/A
CSC-1.104	FAT - Security architecture	0.0	N/A
CSC-1.105	FAT - Security operation	0.0	N/A
CSC-1.106	Several functional areas	0.0	N/A
CSC-1.107	FAT - Risk assessment	0.0	N/A
CSC-1.108	FAT - Physical security	0.0	N/A
CSC-1.109	FAT - Governance	0.0	N/A
CSC-1.110	FAT - Security architecture	0.0	N/A
CSC-1.111	FAT - Security operation	0.0	N/A
CSC-1.112	Several functional areas	0.0	N/A
CSC-1.113	FAT - Risk assessment	0.0	N/A
CSC-1.114	FAT - Physical security	0.0	N/A
CSC-1.115	FAT - Governance	0.0	N/A
CSC-1.116	FAT - Security architecture	0.0	N/A
CSC-1.117	FAT - Security operation	0.0	N/A
CSC-1.118	Several functional areas	0.0	N/A
CSC-1.119	FAT - Risk assessment	0.0	N/A
CSC-1.120	FAT - Physical security	0.0	N/A
CSC-1.121	FAT - Governance	0.0	N/A
CSC-1.122	FAT - Security architecture	0.0	N/A
CSC-1.123	FAT - Security operation	0.0	N/A
CSC-1.124	Several functional areas	0.0	N/A
CSC-1.125	FAT - Risk assessment	0.0	N/A
CSC-1.126	FAT - Physical security	0.0	N/A
CSC-1.127	FAT - Governance	0.0	N/A
CSC-1.128	FAT - Security architecture	0.0	N/A
CSC-1.129	FAT - Security operation	0.0	N/A
CSC-1.130	Several functional areas	0.0	N/A
CSC-1.131	FAT - Risk assessment	0.0	N/A
CSC-1.132	FAT - Physical security	0.0	N/A
CSC-1.133	FAT - Governance	0.0	N/A
CSC-1.134	FAT - Security architecture	0.0	N/A
CSC-1.135	FAT - Security operation	0.0	N/A
CSC-1.136	Several functional areas	0.0	N/A
CSC-1.137	FAT - Risk assessment	0.0	N/A
CSC-1.138	FAT - Physical security	0.0	N/A
CSC-1.139	FAT - Governance	0.0	N/A
CSC-1.140	FAT - Security architecture	0.0	N/A
CSC-1.141	FAT - Security operation	0.0	N/A
CSC-1.142	Several functional areas	0.0	N/A
CSC-1.143	FAT - Risk assessment	0.0	N/A
CSC-1.144	FAT - Physical security	0.0	N/A
CSC-1.145	FAT - Governance	0.0	N/A
CSC-1.146	FAT - Security architecture	0.0	N/A
CSC-1.147	FAT - Security operation	0.0	N/A
CSC-1.148	Several functional areas	0.0	N/A
CSC-1.149	FAT - Risk assessment	0.0	N/A
CSC-1.150	FAT - Physical security	0.0	N/A
CSC-1.151	FAT - Governance	0.0	N/A
CSC-1.152	FAT - Security architecture	0.0	N/A
CSC-1.153	FAT - Security operation	0.0	N/A
CSC-1.154	Several functional areas	0.0	N/A
CSC-1.155	FAT - Risk assessment	0.0	N/A
CSC-1.156	FAT - Physical security	0.0	N/A
CSC-1.157	FAT - Governance	0.0	N/A
CSC-1.158	FAT - Security architecture	0.0	N/A
CSC-1.159	FAT - Security operation	0.0	N/A
CSC-1.160	Several functional areas	0.0	N/A
CSC-1.161	FAT - Risk assessment	0.0	N/A
CSC-1.162	FAT - Physical security	0.0	N/A
CSC-1.163	FAT - Governance	0.0	N/A
CSC-1.164	FAT - Security architecture	0.0	N/A
CSC-1.165	FAT - Security operation	0.0	N/A
CSC-1.166	Several functional areas	0.0	N/A
CSC-1.167	FAT - Risk assessment	0.0	N/A
CSC-1.168	FAT - Physical security	0.0	N/A
CSC-1.169	FAT - Governance	0.0	N/A
CSC-1.170	FAT - Security architecture	0.0	N/A
CSC-1.171	FAT - Security operation	0.0	N/A
CSC-1.172	Several functional areas	0.0	N/A
CSC-1.173	FAT - Risk assessment	0.0	N/A
CSC-1.174	FAT - Physical security	0.0	N/A
CSC-1.175	FAT - Governance	0.0	N/A
CSC-1.176	FAT - Security architecture	0.0	N/A
CSC-1.177	FAT - Security operation	0.0	N/A
CSC-1.178	Several functional areas	0.0	N/A
CSC-1.179	FAT - Risk assessment	0.0	N/A
CSC-1.180	FAT - Physical security	0.0	N/A
CSC-1.181	FAT - Governance	0.0	N/A
CSC-1.182	FAT - Security architecture	0.0	N/A
CSC-1.183	FAT - Security operation	0.0	N/A
CSC-1.184	Several functional areas	0.0	N/A
CSC-1.185	FAT - Risk assessment	0.0	N/A
CSC-1.186	FAT - Physical security	0.0	N/A
CSC-1.187	FAT - Governance	0.0	N/A
CSC-1.188	FAT - Security architecture	0.0	N/A
CSC-1.189	FAT - Security operation	0.0	N/A
CSC-1.190	Several functional areas	0.0	N/A
CSC-1.191	FAT - Risk assessment	0.0	N/A
CSC-1.192	FAT - Physical security	0.0	N/A
CSC-1.193	FAT - Governance	0.0	N/A
CSC-1.194	FAT - Security architecture	0.0	N/A
CSC-1.195	FAT - Security operation	0.0	N/A
CSC-1.196	Several functional areas	0.0	N/A
CSC-1.197	FAT - Risk assessment	0.0	N/A
CSC-1.198	FAT - Physical security	0.0	N/A
CSC-1.199	FAT - Governance	0.0	N/A
CSC-1.200	FAT - Security architecture	0.0	N/A
CSC-1.201	FAT - Security operation	0.0	N/A
CSC-1.202	Several functional areas	0.0	N/A
CSC-1.203	FAT - Risk assessment	0.0	N/A
CSC-1.204	FAT - Physical security	0.0	N/A
CSC-1.205	FAT - Governance	0.0	N/A
CSC-1.206	FAT - Security architecture	0.0	N/A
CSC-1.207	FAT - Security operation	0.0	N/A
CSC-1.208	Several functional areas	0.0	N/A
CSC-1.209	FAT - Risk assessment	0.0	N/A
CSC-1.210	FAT - Physical security	0.0	N/A
CSC-1.211	FAT - Governance	0.0	N/A
CSC-1.212	FAT - Security architecture	0.0	N/A
CSC-1.213	FAT - Security operation	0.0	N/A
CSC-1.214	Several functional areas	0.0	N/A
CSC-1.215	FAT - Risk assessment	0.0	N/A
CSC-1.216	FAT - Physical security	0.0	N/A
CSC-1.217	FAT - Governance	0.0	N/A
CSC-1.218	FAT - Security architecture	0.0	N/A
CSC-1.219	FAT - Security operation	0.0	N/A
CSC-1.220	Several functional areas	0.0	N/A
CSC-1.221	FAT - Risk assessment	0.0	N/A
CSC-1.222	FAT - Physical security	0.0	N/A
CSC-1.223	FAT - Governance	0.0	N/A
CSC-1.224	FAT - Security architecture	0.0	N/A
CSC-1.225	FAT - Security operation	0.0	N/A
CSC-1.226	Several functional areas	0.0	N/A
CSC-1.227	FAT - Risk assessment	0.0	N/A
CSC-1.228	FAT - Physical security	0.0	N/A
CSC-1.229	FAT - Governance	0.0	N/A
CSC-1.230	FAT - Security architecture	0.0	N/A
CSC-1.231	FAT - Security operation	0.0	N/A
CSC-1.232	Several functional areas	0.0	N/A
CSC-1.233	FAT - Risk assessment	0.0	N/A
CSC-1.234	FAT - Physical security	0.0	N/A
CSC-1.235	FAT - Governance	0.0	N/A
CSC-1.236	FAT - Security architecture	0.0	N/A
CSC-1.237	FAT - Security operation	0.0	N/A
CSC-1.238	Several functional areas	0.0	N/A
CSC-1.239	FAT - Risk assessment	0.0	N/A
CSC-1.240	FAT - Physical security	0.0	N/A
CSC-1.241	FAT - Governance	0.0	N/A
CSC-1.242	FAT - Security architecture	0.0	N/A
CSC-1.243	FAT - Security operation	0.0	N/A
CSC-1.244	Several functional areas	0.0	N/A
CSC-1.245	FAT - Risk assessment	0.0	N/A
CSC-1.246	FAT - Physical security	0.0	N/A
CSC-1.247	FAT - Governance	0.0	N/A
CSC-1.248	FAT - Security architecture	0.0	N/A
CSC-1.249	FAT - Security operation	0.0	N/A
CSC-1.250	Several functional areas	0.0	N/A
CSC-1.251	FAT - Risk assessment	0.0	N/A
CSC-1.252	FAT - Physical security	0.0	N/A
CSC-1.253	FAT - Governance	0.0	N/A
CSC-1.254	FAT - Security architecture	0.0	N/A
CSC-1.255	FAT - Security operation	0.0	N/A
CSC-1.256	Several functional areas	0.0	N/A
CSC-1.257	FAT - Risk assessment	0.0	N/A
CSC-1.258	FAT - Physical security	0.0	N/A
CSC-1.259	FAT - Governance	0.0	N/A
CSC-1.260	FAT - Security architecture	0.0	N/A
CSC-1.261	FAT - Security operation	0.0	N/A
CSC-1.262	Several functional areas	0.0	N/A
CSC-1.263	FAT - Risk assessment	0.0	N/A
CSC-1.264	FAT - Physical security	0.0	N/A
CSC-1.265	FAT - Governance	0.0	N/A
CSC-1.266	FAT - Security architecture	0.0	N/A
CSC-1.267	FAT - Security operation	0.0	N/A
CSC-1.268	Several functional areas	0.0	N/A
CSC-1.269	FAT - Risk assessment	0.0	N/A
CSC-1.270	FAT - Physical security	0.0	N/A
CSC-1.271	FAT - Governance	0.0	N/A
CSC-1.272	FAT - Security architecture	0.0	N/A
CSC-1.273	F		

Activo

		Leading functional area	Current status	Constraint operator	Constrains
BUSINESS ASSET					
ID AM	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities	Several functional areas	0.0	N/A	0.0
CSC-1.1	Establish and maintain detailed enterprise asset inventory	Several functional areas	0.0	N/A	0.0
CSC-1.1	Establish and maintain a security awareness program	FA1 - Risk assessment	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data management process	FA3 - User education	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data inventory	FA4 - Application security	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data recovery process	FA5 - Infrastructure security	0.0	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA6 - Governance	0.0	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID GV-1	Organizational cybersecurity policy is established and communicated	FA10 - Security architecture	0.0	N/A	0.0
ID RA-1	Assess vulnerabilities are identified and documented	FA6 - Governance	0.0	N/A	0.0
ID SC	Supply chain risk management	Several functional areas	0.0	N/A	0.0
ID SC-2	Supply chain risk management	FA7 - Risk assessment	0.0	N/A	0.0
ID SC-5	Responses and recovery planning and testing are conducted with suppliers and providers	Several functional areas	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services	FA5 - Infrastructure security	0.0	N/A	0.0
CSC-4.7	Manage default accounts on enterprise assets and software	Several functional areas	0.0	N/A	0.0
CSC-4.7	Use unique passwords	FA10 - Security architecture	0.0	N/A	0.0
PR AC-2	Access permissions and authorizations are issued, managed, verified, revised, 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 issued, 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 communicate with the risk of the transaction	FA10 - Security architecture	0.0	N/A	0.0
PR AT-1	All users are informed and trained	FA10 - Security architecture	0.0	N/A	0.0
PR DS	Data security	Several functional areas	0.0	N/A	0.0
CSC-3.4	Enterprise detection	FA3 - User education	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
ID DS	Information protection processes and procedures	FA10 - Security architecture	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-11.1	Configure automatic session logging on enterprise assets	FA10 - Security architecture	0.0	N/A	0.0
ID PR-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA10 - Security architecture	0.0	N/A	0.0
PR P-11	Cybersecurity is included in human resources practices	FA11 - Career development	0.0	N/A	0.0
PR P-12	Recruits of information are conducted, maintained, and tested	FA10 - Security architecture	0.0	N/A	0.0
PR P-14	Training, development, and retention	FA10 - Security architecture	0.0	N/A	0.0

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

		Leading functional area	Current status	Constraint operator	Constrains
BUSINESS ASSET					
ID AM	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities	Several functional areas	0.0	N/A	0.0
CSC-1.1	Establish and maintain a security awareness program	Several functional areas	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data management process	FA1 - Risk assessment	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data inventory	FA3 - User education	0.0	N/A	0.0
CSC-1.1	Establish and maintain a data recovery process	FA4 - Application security	0.0	N/A	0.0
CSC-1.1	Configure automatic session logging on enterprise assets	FA5 - Infrastructure security	0.0	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA6 - Governance	0.0	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID GV-1	Organizational cybersecurity policy is established and communicated	FA10 - Security architecture	0.0	N/A	0.0
ID RA-1	Assess vulnerabilities are identified and documented	FA6 - Governance	0.0	N/A	0.0
ID SC	Supply chain risk management	Several functional areas	0.0	N/A	0.0
PR AC	Suppliers and partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	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-4.7	Use unique passwords	FA10 - Security architecture	0.0	N/A	0.0
PR AC-2	Access permissions and authorizations are issued, managed, verified, revised, 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 communicate with the risk of the transaction	FA10 - Security architecture	0.0	N/A	0.0
PR AT-1	All users are informed and trained	FA10 - Security architecture	0.0	N/A	0.0
PR DS	Data security	Several functional areas	0.0	N/A	0.0
CSC-3.4	Enterprise detection	FA3 - User education	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
ID DS	Information protection processes and procedures	FA10 - Security architecture	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-11.1	Configure automatic session logging on enterprise assets	FA10 - Security architecture	0.0	N/A	0.0
ID PR-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA10 - Security architecture	0.0	N/A	0.0
PR P-11	Cybersecurity is included in human resources practices	FA11 - Career development	0.0	N/A	0.0
PR P-12	Recruits of information are conducted, maintained, and tested	FA10 - Security architecture	0.0	N/A	0.0
PR P-14	Training, development, and retention	FA10 - Security architecture	0.0	N/A	0.0

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

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 assessment	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 assessment	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	FA5 - Governance	0.0	N/A	0.0
ID DV-1	Organizational cybersecurity policy is established and communicated	FA7 - Risk assessment	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 assessment	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	FA9 - Frameworks and standards	0.0	N/A	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	Several functional areas	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services.	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.7	Identity management, authentication and access control	FA10 - Security architecture	0.0	N/A	0.0
CSC-5.2	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
PR AC-1	Use unique passwords	FA10 - Security architecture	0.0	N/A	0.0
PR AC-3	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-4	Remote access is managed	FA10 - Security architecture	0.0	N/A	0.0
PR AC-5	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-6	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	FA3 - User education	0.0	N/A	0.0
PR AT-1	All users are informed and trained	FA10 - Security architecture	0.0	N/A	0.0
PR DS	Data security	FA10 - Security architecture	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	FA10 - Security architecture	0.0	N/A	0.0
9D-9	Degree of defense	FA10 - Security architecture	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	FA10 - Security architecture	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 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

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 assessment	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	FA7 - Risk assessment	0.0	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA8 - Application security	0.0	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID GV	Governance	FA10 - Security architecture	0.0	N/A	0.0
ID DV-1	Organizational cybersecurity policy is established and communicated	FA5 - Governance	0.0	N/A	0.0
ID RA	Risk assessment	FA7 - Risk assessment	0.0	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA7 - Risk assessment	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	FA9 - Frameworks and standards	0.0	N/A	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	Several functional areas	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services.	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.7	Identity management, authentication and access control	FA10 - Security architecture	0.0	N/A	0.0
CSC-5.2	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
PR AC-1	Use unique passwords	FA10 - Security architecture	0.0	N/A	0.0
PR AC-3	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-4	Remote access is managed	FA10 - Security architecture	0.0	N/A	0.0
PR AC-5	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-6	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	FA3 - User education	0.0	N/A	0.0
PR AT-1	All users are informed and trained	FA10 - Security architecture	0.0	N/A	0.0
PR DS	Data security	FA10 - Security architecture	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	FA10 - Security architecture	0.0	N/A	0.0
9D-9	Degree 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	FA11 - Career development	0.0	N/A	0.0
PR IP-11	Cybersecurity is included in human resources practices	FA10 - Security architecture	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

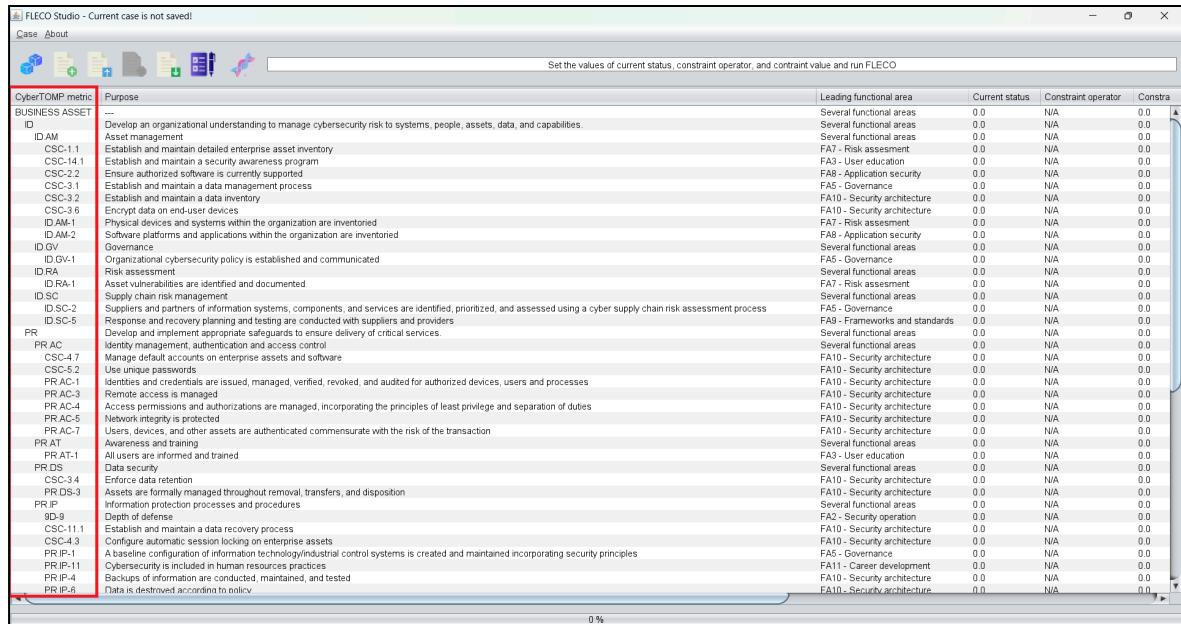
Figura 10. Análisis las actuaciones de ciberseguridad de un activo

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



The screenshot shows the FLECO Studio interface with the title bar "FLECO Studio - Current case is not saved!" and menu items "Case" and "About". Below the menu is a toolbar with icons for file operations. The main area displays a table titled "CyberTOMP metric" with the following columns: "Purpose", "Leading functional area", "Current status", "Constraint operator", and "Constra". The table lists various cybersecurity requirements and their corresponding functional areas and current status values. A red box highlights the "Purpose" column.

	Purpose	Leading functional area	Current status	Constraint operator	Constra
BUSINESS ASSET		Several functional areas	0.0	N/A	0.0
ID AM	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.0	N/A	0.0
CSC-1.1	Asset management	Several functional areas	0.0	N/A	0.0
CSC-14.1	Establish and maintain detailed enterprise asset inventory	FAT - Risk assessment	0.0	N/A	0.0
CSC-2.2	Establish and maintain a security awareness program	FA3 - User education	0.0	N/A	0.0
CSC-3.1	Ensure authorized software is currently supported	FA8 - Application security	0.0	N/A	0.0
CSC-3.2	Establish and maintain a data management process	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.3	Establish and maintain a data inventory	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.4	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	FA10 - Security architecture	0.0	N/A	0.0
ID AM-2	Software, platforms, and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID GOV	Governance	FA10 - Security architecture	0.0	N/A	0.0
ID GV-1	Organizational cybersecurity policy is established and communicated	FA10 - Security architecture	0.0	N/A	0.0
ID RA	Risk assessment	FA10 - Security architecture	0.0	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA10 - Security architecture	0.0	N/A	0.0
ID SC	Supply chain risk management	FA10 - Security architecture	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	FA10 - Security architecture	0.0	N/A	0.0
ID SC-5	Procurement and vendor management testing are conducted with suppliers and providers	FA10 - Security architecture	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services.	FA10 - Security architecture	0.0	N/A	0.0
PR AC-1	Identity management, authentication and access control	FA10 - Security architecture	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	Multi-factor authentication 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	FA10 - Security architecture	0.0	N/A	0.0
PR AT-1	All users are informed and trained	FA10 - Security architecture	0.0	N/A	0.0
PR DS	Data security	FA10 - Security architecture	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 DS-4	Information protection processes and procedures	FA10 - Security architecture	0.0	N/A	0.0
ID R	Depth of recovery	FA10 - Security architecture	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	FA10 - Security architecture	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

CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET						
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.					
CSC-11	Establish and maintain a detailed enterprise asset inventory	Several functional areas	0.0	N/A	0.0	
CSC-14	Establish and maintain a security awareness program	Several functional areas	0.0	N/A	0.0	
CSC-22	Ensure authorized software is currently supported	Several functional areas	0.0	N/A	0.0	
CSC-31	Establish and maintain a data management process	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-32	Establish and maintain a data inventory	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-36	Encrypt data at rest and in transit	FA1 - Risk assessment	0.0	N/A	0.0	
ID AM-1	Physical devices and systems within the organization are inventoried	FA1 - Risk assessment	0.0	N/A	0.0	
ID AM-2	Software platforms and applications within the organization are inventoried	FA1 - Risk assessment	0.0	N/A	0.0	
ID GV	Governance	FA1 - Risk assessment	0.0	N/A	0.0	
ID GV-1	Organizational cybersecurity policy is established and communicated	Several functional areas	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	Several functional areas	0.0	N/A	0.0	
ID SC	Supply chain risk management	FA1 - Risk assessment	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	Several functional areas	0.0	N/A	0.0	
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA1 - Risk assessment	0.0	N/A	0.0	
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	FA1 - Risk assessment	0.0	N/A	0.0	
PR AC	Identity management, authentication and access control	FA1 - Risk assessment	0.0	N/A	0.0	
PR AC-17	Manage default accounts on enterprise assets and software	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-4	Use unique passwords	FA1 - Risk assessment	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	FA1 - Security architecture	0.0	N/A	0.0	
PR AC-3	Remote access is managed	FA1 - 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	FA1 - Security architecture	0.0	N/A	0.0	
PR AC-5	Network integrity is protected	FA1 - Security architecture	0.0	N/A	0.0	
PR AC-6	Users, devices, and other assets are authenticated commensurate with the risk of the transaction	FA1 - Security architecture	0.0	N/A	0.0	
PR AT	Awareness and training	FA1 - Security architecture	0.0	N/A	0.0	
PR AT-1	All users are informed and trained	FA1 - Security architecture	0.0	N/A	0.0	
PR DS	Data security	FA1 - Security architecture	0.0	N/A	0.0	
CSC-34	Enforce data retention	FA1 - Security architecture	0.0	N/A	0.0	
PR DS-3	Assets are formally managed throughout removal, transfers, and disposition	FA1 - Security architecture	0.0	N/A	0.0	
PR DS-9	Depth of defense	FA1 - Security architecture	0.0	N/A	0.0	
CSC-11	Establish and maintain a data recovery process	FA1 - Security architecture	0.0	N/A	0.0	
CSC-43	Configure automatic session locking on enterprise assets	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-11	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-4	Cybersecurity is included in human resources practices	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-6	Backups of information are conducted, maintained, and tested	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-9	Data is destroyed according to policy	FA1 - Security architecture	0.0	N/A	0.0	
PR MA	Response plan (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FA1 - Security architecture	0.0	N/A	0.0	
CSC-12.1	Maintain a secure network infrastructure	FA1 - Security architecture	0.0	N/A	0.0	
CSC-4.2	Establish and maintain a secure configuration process for network infrastructure	FA1 - Security architecture	0.0	N/A	0.0	
CSC-4.6	Securely manage enterprise assets and software	FA1 - Security architecture	0.0	N/A	0.0	
CSC-7.3	Perform automated operating system patch management	FA1 - Security architecture	0.0	N/A	0.0	
CSC-8.1	Establish and maintain an audit log management process	FA1 - Governance	0.0	N/A	0.0	

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

CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET						
ID	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.					
CSC-11	Establish and maintain a detailed enterprise asset inventory	Several functional areas	0.0	N/A	0.0	
CSC-14	Establish and maintain a security awareness program	Several functional areas	0.0	N/A	0.0	
CSC-22	Ensure authorized software is currently supported	Several functional areas	0.0	N/A	0.0	
CSC-31	Establish and maintain a data management process	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-32	Establish and maintain a data inventory	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-36	Encrypt data at rest and in transit	FA1 - Risk assessment	0.0	N/A	0.0	
ID AM-1	Physical devices and systems within the organization are inventoried	FA1 - Risk assessment	0.0	N/A	0.0	
ID AM-2	Software platforms and applications within the organization are inventoried	FA1 - Risk assessment	0.0	N/A	0.0	
ID GV	Governance	FA1 - Risk assessment	0.0	N/A	0.0	
ID GV-1	Organizational cybersecurity policy is established and communicated	Several functional areas	0.0	N/A	0.0	
ID RA	Risk assessment	FA1 - Risk assessment	0.0	N/A	0.0	
ID RA-1	Asset vulnerabilities are identified and documented	Several functional areas	0.0	N/A	0.0	
ID SC	Supply chain risk management	FA1 - Risk assessment	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	Several functional areas	0.0	N/A	0.0	
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	FA1 - Risk assessment	0.0	N/A	0.0	
PR AC	Identity management, authentication and access control	FA1 - Risk assessment	0.0	N/A	0.0	
PR AC-17	Manage default accounts on enterprise assets and software	FA1 - Risk assessment	0.0	N/A	0.0	
CSC-4	Use unique passwords	FA1 - Risk assessment	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	FA1 - Security architecture	0.0	N/A	0.0	
PR AC-3	Remote access is managed	FA1 - 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	FA1 - Security architecture	0.0	N/A	0.0	
PR AC-5	Network integrity is protected	FA1 - 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	FA1 - Security architecture	0.0	N/A	0.0	
PR AT	Awareness and training	FA1 - Security architecture	0.0	N/A	0.0	
PR AT-1	All users are informed and trained	FA1 - Security architecture	0.0	N/A	0.0	
PR DS	Data security	FA1 - Security architecture	0.0	N/A	0.0	
CSC-34	Enforce data retention	FA1 - Security architecture	0.0	N/A	0.0	
PR DS-3	Assets are formally managed throughout removal, transfers, and disposition	FA1 - Security architecture	0.0	N/A	0.0	
PR DS-9	Depth of defense	FA1 - Security architecture	0.0	N/A	0.0	
CSC-11.1	Establish and maintain a data recovery process	FA1 - Security architecture	0.0	N/A	0.0	
CSC-4.3	Configure automatic session locking on enterprise assets	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-11	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-4	Cybersecurity is included in human resources practices	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-6	Backups of information are conducted, maintained, and tested	FA1 - Security architecture	0.0	N/A	0.0	
PR IP-9	Data is destroyed according to policy	FA1 - Security architecture	0.0	N/A	0.0	
PR MA	Response plan (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FA1 - Security architecture	0.0	N/A	0.0	
CSC-12.1	Maintain a secure network infrastructure	FA1 - Security architecture	0.0	N/A	0.0	
CSC-4.2	Establish and maintain a secure configuration process for network infrastructure	FA1 - Security architecture	0.0	N/A	0.0	
CSC-4.6	Securely manage enterprise assets and software	FA1 - Security architecture	0.0	N/A	0.0	
CSC-7.3	Perform automated operating system patch management	FA1 - Security architecture	0.0	N/A	0.0	
CSC-8.1	Establish and maintain an audit log management process	FA1 - Governance	0.0	N/A	0.0	

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

CyberTOMP metric Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET					
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	Several functional areas	0.0	N/A	0.0
CSC-1.4	Establish and maintain a security awareness program	Several functional areas	0.0	N/A	0.0
CSC-2.2	Ensure authorized software is currently supported	Several functional areas	0.0	N/A	0.0
CSC-3.1	Establish and maintain a data management process	FA7 - Risk assessment	0.0	N/A	0.0
CSC-3.2	Establish and maintain a data inventory	FA8 - Application security	0.0	N/A	0.0
CSC-3.6	Encrypt data on end-user devices	FA9 - Security architecture	0.0	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID DV	Governance	FA10 - Security architecture	0.0	N/A	0.0
ID GV-1	Organizational cybersecurity policy is established and communicated	FA10 - Security architecture	0.0	N/A	0.0
ID RA	Risk assessment	FA10 - Security architecture	0.0	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA10 - Security architecture	0.0	N/A	0.0
ID SC	Supply chain risk management	FA10 - Security architecture	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	FA10 - Security architecture	0.0	N/A	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA10 - Security architecture	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.0	N/A	0.0
PR AC-1	Identity management, authentication and access control	Several functional areas	0.0	N/A	0.0
CSC-3.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.8	User 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-5	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-7	Network integrity is protected	FA10 - Security architecture	0.0	N/A	0.0
PR AC-8	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 protection	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	FA10 - Security architecture	0.0	N/A	0.0
PR IP-11	Cybersecurity is included in human resources practices	FA5 - Governance	0.0	N/A	0.0
PR IP-4	Backups of information are conducted, maintained, and tested	FA11 - Career development	0.0	N/A	0.0
PR IP-6	Data is destroyed according to policy	FA10 - Security architecture	0.0	N/A	0.0
PR IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FA5 - Governance	0.0	N/A	0.0
PR MA	Maintenance	Several functional areas	0.0	N/A	0.0
CSC-1.2.1	Ensure network infrastructure is up-to-date	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.2	Establish and maintain a secure configuration process for network infrastructure	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.6	Securely manage enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
CSC-7.3	Perform automated operating system patch management	FA10 - Security architecture	0.0	N/A	0.0
CSC-7.1	Establish and maintain an audit log management process	FA5 - Governance	0.0	N/A	0.0

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

CyberTOMP metric Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET					
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	Several functional areas	0.0	N/A	0.0
CSC-14	Establish and maintain a security awareness program	Several functional areas	0.0	N/A	0.0
CSC-2.2	Ensure authorized software is currently supported	FA7 - Risk assessment	0.0	N/A	0.0
CSC-3.1	Establish and maintain a data management process	FA3 - User education	0.0	N/A	0.0
CSC-3.2	Establish and maintain a data inventory	FA8 - Application security	0.0	N/A	0.0
CSC-3.6	Encrypt data on end-user devices	FA9 - Security architecture	0.0	N/A	0.0
ID AM-1	Physical devices and systems within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID AM-2	Software platforms and applications within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0
ID DV	Governance	FA10 - Security architecture	0.0	N/A	0.0
ID GV-1	Organizational cybersecurity policy is established and communicated	FA10 - Security architecture	0.0	N/A	0.0
ID RA	Risk assessment	FA10 - Security architecture	0.0	N/A	0.0
ID RA-1	Asset vulnerabilities are identified and documented	FA10 - Security architecture	0.0	N/A	0.0
ID SC	Supply chain risk management	FA10 - Security architecture	0.0	N/A	0.0
ID SC-5	Response and recovery planning and testing are conducted with suppliers and providers	FA10 - Security architecture	0.0	N/A	0.0
PR AC	Develop and implement appropriate safeguards to ensure delivery of critical services.	Several functional areas	0.0	N/A	0.0
PR AC-1	Identity management, authentication and access control	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.7	Manage default accounts on enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
CSC-3.8	User 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-5	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-7	Network integrity is protected	FA10 - Security architecture	0.0	N/A	0.0
PR AC-8	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 protection	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
PR IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FA5 - Governance	0.0	N/A	0.0
PR MA	Maintenance	Several functional areas	0.0	N/A	0.0
CSC-12.1	Ensure network infrastructure is up-to-date	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.2	Establish and maintain a secure configuration process for network infrastructure	FA10 - Security architecture	0.0	N/A	0.0
CSC-4.6	Securely manage enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0
CSC-7.3	Perform automated operating system patch management	FA10 - Security architecture	0.0	N/A	0.0
CSC-7.1	Establish and maintain an audit log management process	FA5 - Governance	0.0	N/A	0.0

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

Set the values of current status, constraint operator, and constraint value and run FLECO						
CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET	---	Several functional areas	0.0	N/A	0.0	
ID_AM	Develop an organization's understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Several functional areas	0.0	N/A	0.0	
CSC-1.1	Establish and maintain detailed enterprise asset inventory	Several functional areas	0.0	N/A	0.0	
CSC-14.1	Establish and maintain a security awareness program	FAT - Risk assessment	0.0	N/A	0.0	
CSC-2.2	Ensure authorized software is currently supported	FA3 - User education	0.0	N/A	0.0	
CSC-3.1	Establish and maintain a data management process	FA8 - Application security	0.0	N/A	0.0	
CSC-3.2	Establish and maintain a data inventory	FAT5 - Governance	0.0	N/A	0.0	
CSC-3.5	Establish and maintain an incident detection system	FA10 - Security architecture	0.0	N/A	0.0	
ID_AM-1	Encrypt devices and systems within the organization are inventoried	FA10 - Security architecture	0.0	N/A	0.0	
ID_AM-2	Software platforms and applications within the organization are inventoried	FA7 - Risk assessment	0.0	N/A	0.0	
ID_GV	Governance	FA8 - Application security	0.0	N/A	0.0	
ID_GV-1	Organizational cybersecurity policy is established and communicated	Several functional areas	0.0	N/A	0.0	
ID_RV	Risk assessment	FAT - Governance	0.0	N/A	0.0	
ID_RA-1	Asset vulnerabilities are identified and documented	Several functional areas	0.0	N/A	0.0	
ID_SC	Supply chain risk management	FAT7 - Risk assessment	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	Several functional areas	0.0	N/A	0.0	
ID_SC-5	Response and recovery plans are developed and tested with suppliers and providers	FAT9 - Frameworks and standards	0.0	N/A	0.0	
PR	PR.AC Devise and implement strategies to ensure delivery of critical services.	Several functional areas	0.0	N/A	0.0	
PR.AC	Identity management, authentication and access control	FA10 - Security architecture	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-2	Accesses are 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	FAT3 - Training	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	
ID_IP	Design of information protection	FAT2 - Policy and strategy	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	FA10 - Security architecture	0.0	N/A	0.0	
PR.IP-11	Cybersecurity is included in vendor resources practices	FAT5 - Governance	0.0	N/A	0.0	
PR.IP-4	Baseline of assets are conducted, maintained, and tested	FA11 - Career development	0.0	N/A	0.0	
PR.IP-6	Data is destroyed according to policy	FA10 - Security architecture	0.0	N/A	0.0	
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FAT5 - Governance	0.0	N/A	0.0	
PR.MA	Maintenance	Several functional areas	0.0	N/A	0.0	
CSC-12.1	Ensure network infrastructure is up-to-date	FA10 - Security architecture	0.0	N/A	0.0	
CSC-4.6	Establish and maintain a secure configuration process for network infrastructure	FA10 - Security architecture	0.0	N/A	0.0	
CSC-4.6	Securely manage enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0	
CSC-7.3	Perform automated operating system patch management	FA10 - Security architecture	0.0	N/A	0.0	
CSC-8.1	Establish and maintain an audit log management process	FA10 - Security architecture	0.0	N/A	0.0	
		FAT5 - Governance	0.0	N/A	0.0	

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

Set the values of current status, constraint operator, and constraint value and run FLECO						
CyberTOMP metric	Purpose	Leading functional area	Current status	Constraint operator	Constraint value	Target status
BUSINESS ASSET ...	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	Several functional areas	0.0	N/A	0.0	
CSC-1.4	Establish and maintain a security awareness program	FAT - Functional assessment	0.0	N/A	0.0	
CSC-2.2	Ensure authorized software is currently supported	FA3 - User education	0.0	N/A	0.0	
CSC-3.1	Establish and maintain a data management process	FA4 - Application security	0.0	N/A	0.0	
CSC-3.2	Establish and maintain a data inventory	FA5 - Governance	0.0	N/A	0.0	
CSC-3.6	Encrypt data at 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 assessment	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	FAT - Functional assessment	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-2	Role-based 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	FA4 - User education	0.0	N/A	0.0	
PR.DS	Data protection	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	Several functional areas	0.0	N/A	0.0	
PR.IP	Information protection processes and procedures	FA10 - Security architecture	0.0	N/A	0.0	
9D-9	Design of devices and systems	FA10 - Security architecture	0.0	N/A	0.0	
CSC-1.11	Establish and maintain a data recovery process	Several functional areas	0.0	N/A	0.0	
CSC-4.3	Configure automatic session locking on enterprise assets	FA2 - Security operation	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	FA10 - Security architecture	0.0	N/A	0.0	
PR.IP-11	Cybersecurity is included in human resources practices	FA5 - Governance	0.0	N/A	0.0	
PR.IP-4	Backups of information are conducted, maintained, and tested	FA11 - Career development	0.0	N/A	0.0	
PR.IP-6	Data is destroyed according to policy	FA10 - Security architecture	0.0	N/A	0.0	
PR.RP	Resilience (incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	FA5 - Governance	0.0	N/A	0.0	
PR.MA	Maintenance	Several functional areas	0.0	N/A	0.0	
CSC-1.21	Ensure network infrastructure is up-to-date	FA10 - Security architecture	0.0	N/A	0.0	
CSC-4.2	Establish and maintain a secure configuration process for network infrastructure	FA5 - Governance	0.0	N/A	0.0	
CSC-4.6	Secure manage enterprise assets and software	FA10 - Security architecture	0.0	N/A	0.0	
CSC-7.3	Perform automated operating system patch management	FA10 - Security architecture	0.0	N/A	0.0	
CSC-8.1	Establish and maintain an audit log management process	FA5 - Governance	0.0	N/A	0.0	

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

Manual de uso Fleco Studio © 2024 by José Antonio Bravo Romero y Guadalupe González Santos is licensed under Creative Commons Attribution-ShareAlike 4.0 International. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>



CC BY-SA 4.0

Creative Commons Attribution-ShareAlike 4.0 International

This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, even for commercial purposes. If others remix, adapt, or build upon the material, they must license the modified material under identical terms.

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>