Convocatoria Colaboración Público-Privada CPP2021-009025

DICYME:

Dynamic Industrial CYberrisk Modelling based on Evidence

Iniciativa Conjunta de:

ENTREGABLE 4.2:

Primer Prototipo del Sistema Completo e

Informe de Resultados de Prueba

Coordinadores:

Romy R. Ravines (DeNexus Tech)

Isaac Martín de Diego (Universidad Rey Juan Carlos)

Alberto Fernández Isabel (Universidad Rey Juan Carlos)

Contenido

1 Introducción

En este documento se describe como será el sistema completo que integrará los indicadores y modelos diseñados en DICYME con DeRISK™, que es el objetivo último del proyecto según se explica en la memoria técnica (véase la Ilustración 1. Relación entre DICYME y el sistema de modelos de DeNexus (DeRISK) según la memoria técnica del Proyecto). Como se explica en el entregable E4.1, con la finalidad de disponer de un producto *end-to-end* (E2E) que sea publicado como *web app* de DICYME, y proporcione una solución completa de cálculo del impacto financiero del riesgo cibernético, se usará un sistema alternativo a DeRISK.

De esta manera se mostrará cómo funcionan las sugerencias derivadas de DICYME en el cálculo del ciber riesgo y el sistema de recomendación sin depender del acceso al código fuente del producto DeRISK que es confidencial, propiedad exclusiva de DeNexus, al cual los investigadores de DICYME no pueden acceder. Por otro lado, si el equipo de desarrollo interno de DeNexus consigue integrar las propuestas de DICYME en DeRISK, se elaborará un informe con resultados.

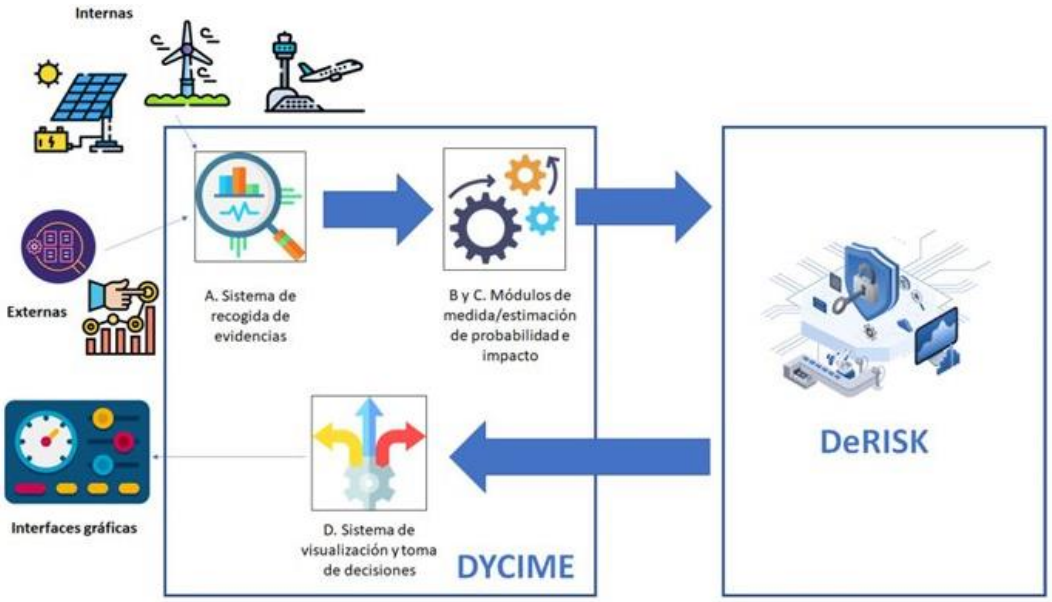


Ilustración 1. Relación entre DICYME y el sistema de modelos de DeNexus (DeRISK) según la memoria técnica del Proyecto

2 El Sistema

Como se ha comentado en la sección anterior, el resultado de DICYME será utilizado por DeNexus dentro de su producto DeRISK. Sin embargo, esta línea de integración escapa al control y alcance de trabajo del equipo del Proyecto. Por este motivo, de aquí en adelante, el Sistema al que nos referimos corresponde al presentado en la Ilustración 2. Marco de Trabajo del Proyecto DICYME. dentro del recuadro gris.

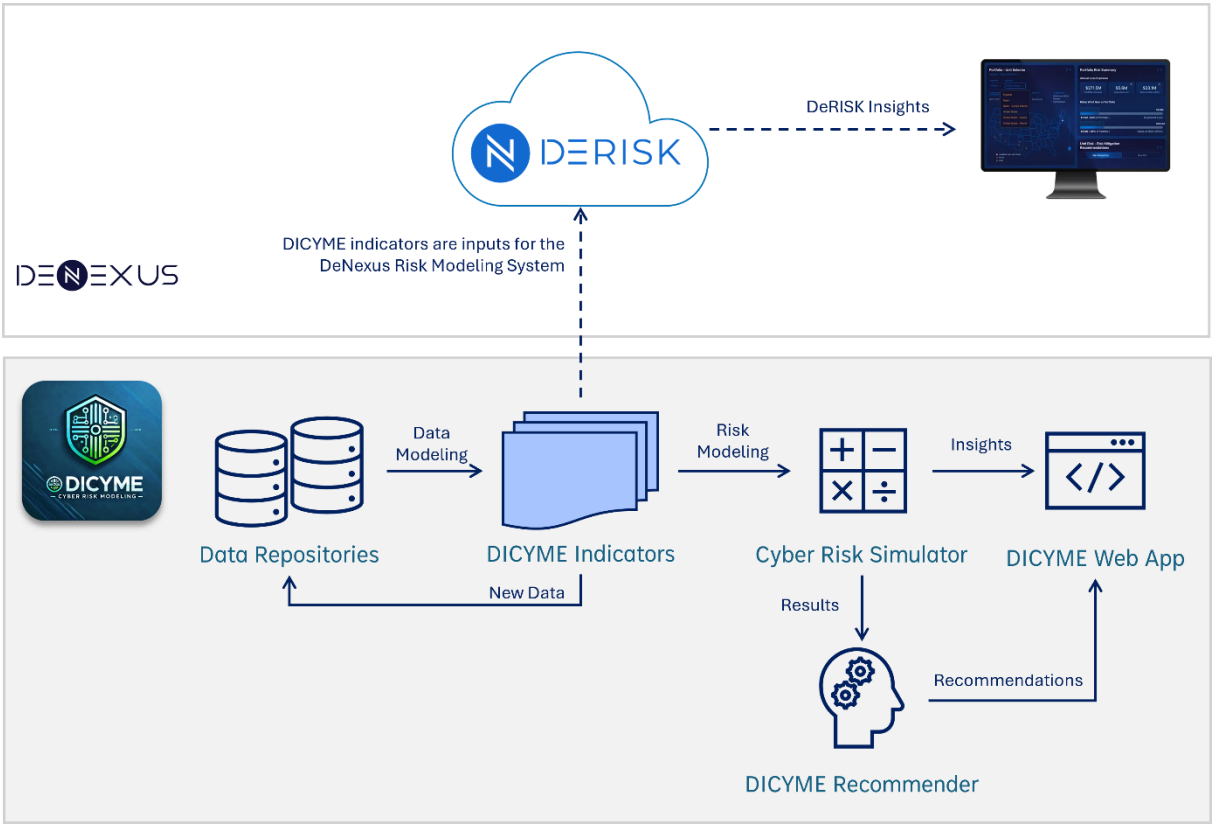


Ilustración 2. Marco de Trabajo del Proyecto DICYME.

Los principales componentes del Sistema DICYME son:

1. Repositorio de datos
2. Indicadores DICYME
3. Simulador de ciberriesgo
4. Recomendador DICYME
5. Aplicación web

Es importante resaltar que el sistema DICYME se encuentra aún en desarrollo y en este entregable se describe un primer prototipo muy preliminar del mismo. El contenido descrito a continuación está sujeto a modificaciones según que vaya concretizando el desarrollo de la aplicación DICYME.

2.1 Repositorio de datos

Como ya se adelantó en el entregable E4.1 y se viene demostrando en sucesivos entregables de otras actividades, una de las principales contribuciones de DICYME es la **recolección automática de datos** con información sobre factores o *drivers* del ciberriesgo. Para ello, se han implementado procesos específicos de recolección adaptados a cada fuente, con los datos almacenados en una base de datos MongoDB en los servidores de la URJC.

Por el momento se ha continuado extrayendo y actualizando el repositorio de datos con los mismos tipos de datos, así como generando relaciones necesarias para el desarrollo de otros sistemas como la aplicación web del proyecto, para la cual se han

relacionado, por ejemplo, las tácticas y técnicas de MITRE entre sí siguiendo la matriz MITRE ATT&CK.

El código y la infraestructura relacionados con la recolección de datos están alojados en repositorios privados del proyecto en GitHub y GitLab, mientras que el almacenamiento y procesamiento se realiza en servidores de la URJC. Además, la aplicación web correspondiente, que integra estos datos y módulos de otras actividades del proyecto, ya está disponible a través de https://gondor.etsii.urjc.es:3866/.

2.2 Indicadores DICYME

En el entregable E4.1 se destacó como segunda gran contribución de DICYME el diseño e implementación de indicadores innovadores para evaluar el ciberriesgo industrial. Este módulo integra subsistemas independientes, cada uno con objetivos específicos, metodologías propias y repositorios de datos, transformando información recolectada en métricas dinámicas que reflejan aspectos clave del perfil de riesgo de las organizaciones.

Los indicadores desarrollados son los ya mencionados en el E4.1: **ATR2ATK**, que mide el atractivo de una organización para ciberataques; **CVE2ATK**, que relaciona vulnerabilidades con técnicas explotables según MITRE ATT&CK; y **THRACT**, que evalúa la evolución de actores de amenazas frente a objetivos específicos. Sin embargo, se han actualizado y mejorado los modelos, incorporando nueva información obtenida del módulo de recolección automática descrito previamente, con el fin de incrementar la precisión y relevancia de los resultados.

2.3 Simulador de ciber riesgo

Este módulo constituye el motor de cálculo de ciber riesgo en DICYME, reemplazando al sistema DeRISK debido a restricciones de acceso previamente explicadas. Basado en una adaptación de la metodología FAIR (véase la Ilustración 3. Taxonomía a alto nivel del enfoque FAIR), simula la frecuencia e impacto de ciber incidentes utilizando distribuciones de probabilidad que, en esta versión, ya incorporan los resultados de algunos de los indicadores desarrollados en el proyecto. El funcionamiento detallado de este simulador con la primera integración de algunos indicadores se describe en la Funcionamiento del Sistema, donde también se exploran posibles escenarios y recomendaciones para la mitigación del riesgo.

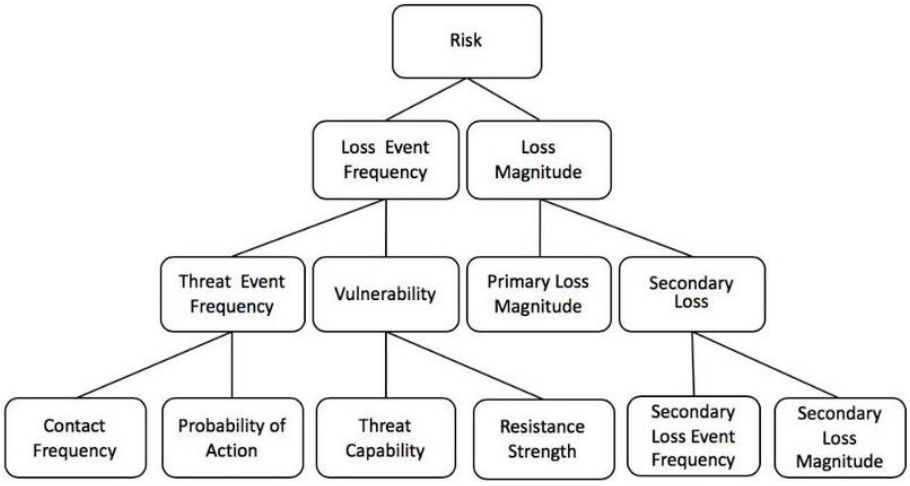


Ilustración 3. Taxonomía a alto nivel del enfoque FAIR

2.4 Recomendador DICYME

Actualmente, no es posible proporcionar detalles sobre el alcance o los propósitos específicos del sistema de recomendación de DICYME, ya que aún no se ha definido con claridad en qué aspectos se centrará. Este módulo está pendiente de desarrollo, y su diseño dependerá de decisiones futuras relacionadas con las prioridades del proyecto y las necesidades identificadas en etapas posteriores. Su implementación será abordada en los próximos entregables, donde se establecerán sus objetivos concretos y funcionalidades.

2.5 Aplicación web

La aplicación web es el nombre que usamos para el sistema de visualización y herramienta de recomendaciones que se cita en la memoria técnica de DICYME. Esta aplicación se está desarrollando y está alojada en los servidores de la URJC, accesible públicamente en https://gondor.etsii.urjc.es:3866/. En el entregable E3.1 se describe el trabajo realizado hasta junio 2024, y en el entregable E3.2 se incluirán avances en los que ya se está trabajando.

Además, esta aplicación incluye el trabajo desarrollado en esta actividad 4, dadas las limitaciones de integración directa con DeRisk ya descritos. La novedad de esta línea de trabajo es que dicha herramienta será independiente de DeRISK, incluyendo un motor de cálculo sencillo pero eficaz, basado en la metodología FAIR.

3 Funcionamiento del Sistema

La Ilustración 4. Esquema de Funcionamiento del Sistema DICYME recuerda el funcionamiento a alto nivel del sistema, que puede interpretarse como un flujo de datos donde en cada paso se ejecutan múltiples procesos que transforman el dato recibido en información de apoyo a la toma de decisiones.

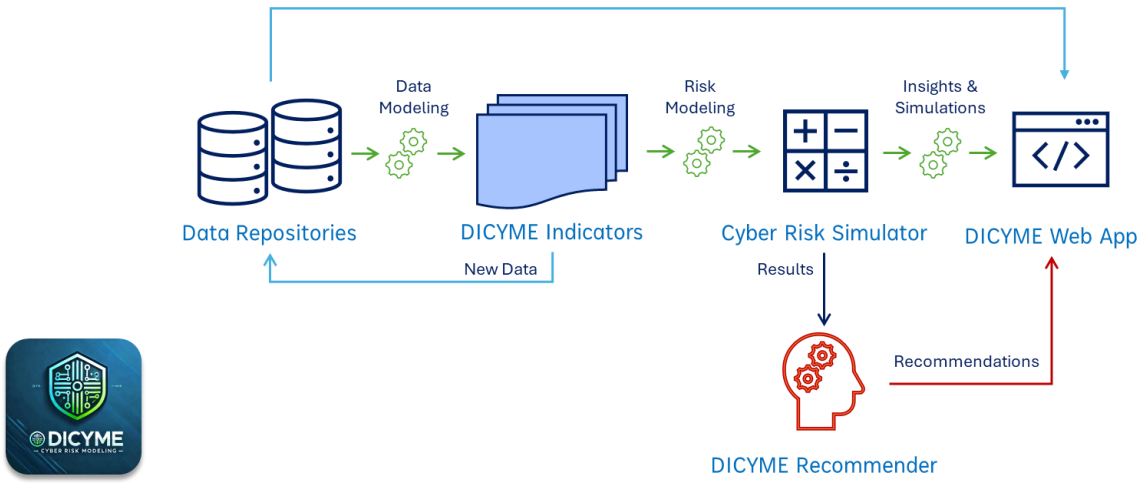


Ilustración 4. Esquema de Funcionamiento del Sistema DICYME

En este primer prototipo se ha trabajado en una primera aproximación que incluye resultados de algunos de los modelos del proyecto. En concreto, se emplean ATR2ATK y THRACT para estimar el nodo de frecuencia de eventos de amenazas. De momento, únicamente se puede calcular el ciber riesgo para las compañías presentes en el

conjunto de datos de perfil de víctimas desarrollado en la actividad 1. Sin embargo, como se está trabajando paralelamente en añadir la ejecución de los diferentes modelos al Sistema, este funcionamiento cambiará, pudiendo realizar una ejecución *end-to*-end para una compañía dadas sus características, ejecutando los modelos y combinándolos en la estimación del ciber riesgo.

Una vez seleccionada una compañía en el margen izquierdo, el sistema calcula la frecuencia de contacto y la probabilidad de acción. La primera corresponde al valor de atractivo, es decir, la salida del modelo ATR2ATK, en forma de probabilidad entre 0 y 1. La segunda es el valor medio de TRACT para todos los actores de amenaza que tienen entre sus países objetivo el país de la compañía seleccionada, así como la categoría de industria entre sus sectores objetivo. En caso desconocido, principalmente si no hay ningún actor de amenazas que cumpla dichas condiciones, se asigna una puntuación de 0.5. Para que el árbol sea más visual, el nodo es de color naranja si el valor es de 0.5 o superior, y azul en caso contrario.

Tomando ambos resultados, se obtiene la frecuencia de eventos de amenaza empleando la operación del producto. La Ilustración 5. Módulo de cálculo del ciberriesgo del Sistema muestra el árbol al que se hace mención, basado en la metodología FAIR, así como el selector de compañías en el margen izquierdo.

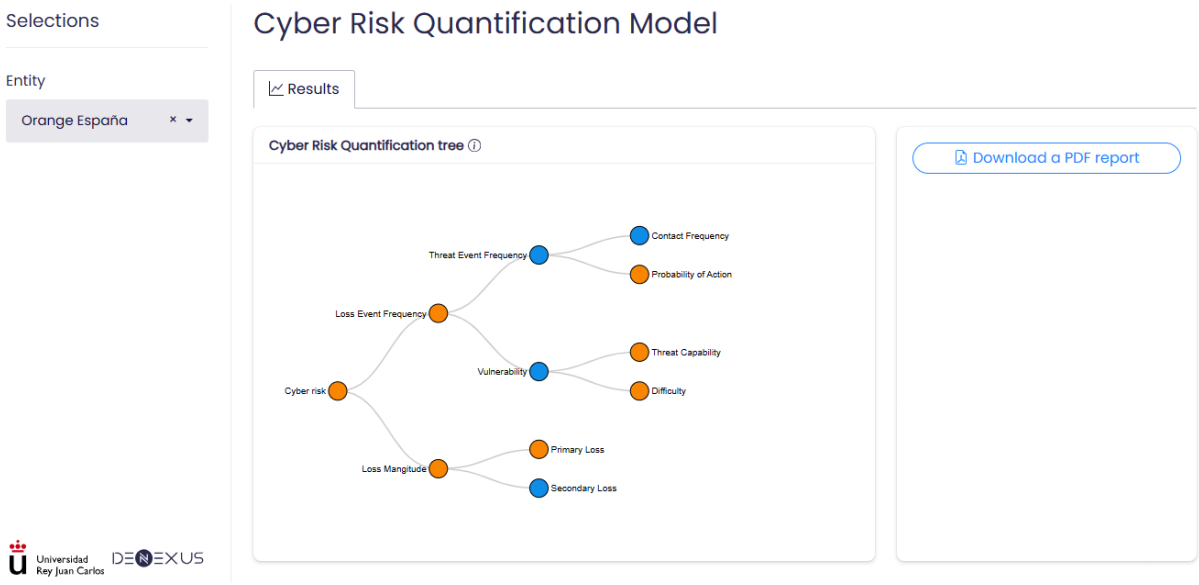


Ilustración 5. Módulo de cálculo del ciberriesgo del Sistema

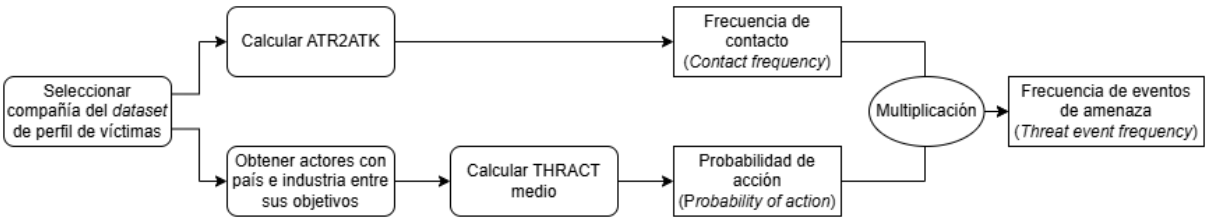


Ilustración 6. Diagrama del cálculo de la frecuencia de eventos de amenaza

Aunque aún quedan ramas del árbol pendientes de definir, ya se está trabajando en una propuesta que permita estimar el impacto de los eventos de amenaza empleando el resto de modelos de DICYME. En la Ilustración 7. Combinación de CWE y MITRE partiendo de escenarios de ataque se muestra una base empleada para esta labor. Dicho diagrama muestra cómo, partiendo de diversas situaciones concretas representadas por

los escenarios de ataque (u otras, como por ejemplo las características técnicas de una compañía), se obtienen los indicadores relacionados del modelo **CVE2ATK** (CVEs, y CWEs presentes en los escenarios o compañía, por ejemplo) y se relacionan con, por ejemplo, las técnicas de impacto de MITRE ATT&CK. Este sistema podría, añadiendo la componente temporal inherente al ciber riesgo y la estimación económica de las pérdidas asociadas (empleando un porcentaje de la facturación de la compañía dado el modelo ATR2ATK, por ejemplo), estimar el impacto. Esta idea conceptual se recoge en la Ilustración 8. Idea conceptual para la estimación del impacto en una compañía, aunque es importante resaltar que puede incluir fallos conceptuales, pues aún debe ser concretada para definir las diferentes estimaciones y ponderaciones necesarias, pudiendo pasar después a su desarrollo e implementación en el modelo. La concreción de este concepto será parte de futuros entregables.

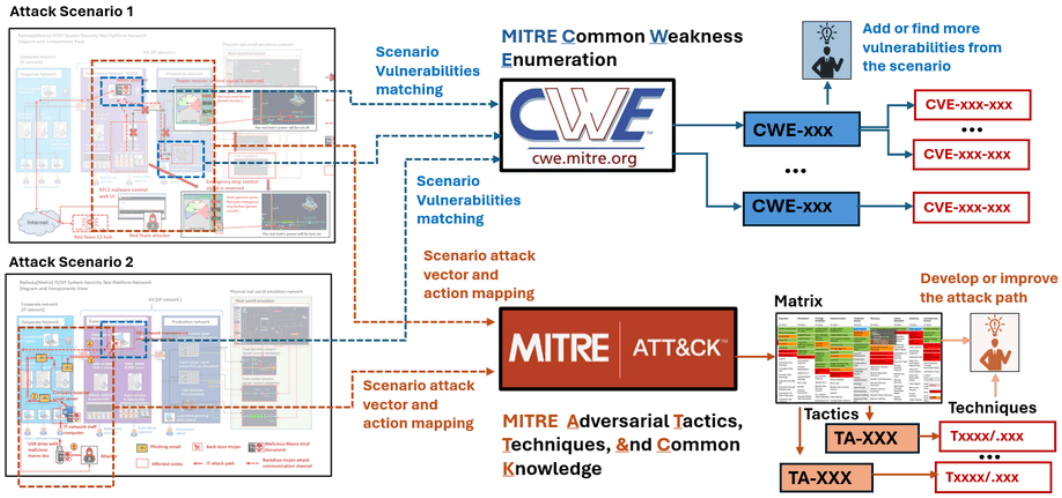


Ilustración 7. Combinación de CWE y MITRE partiendo de escenarios de ataque

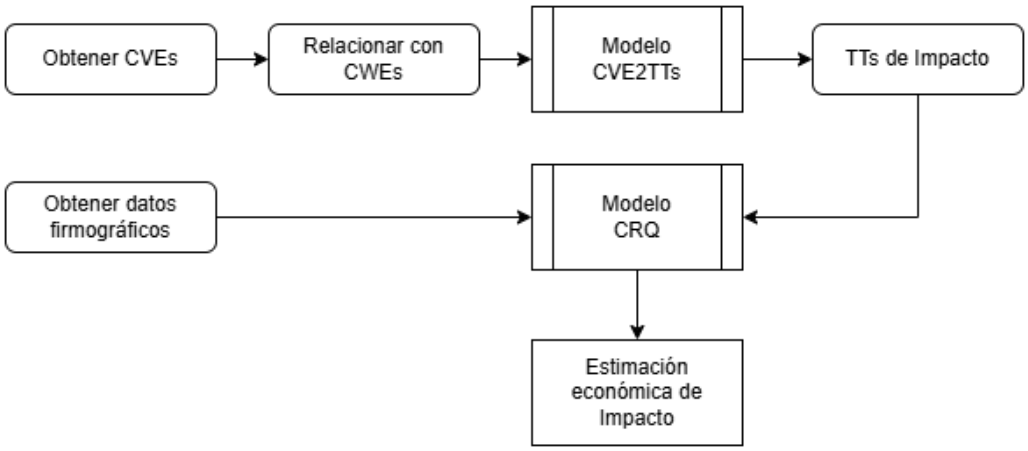


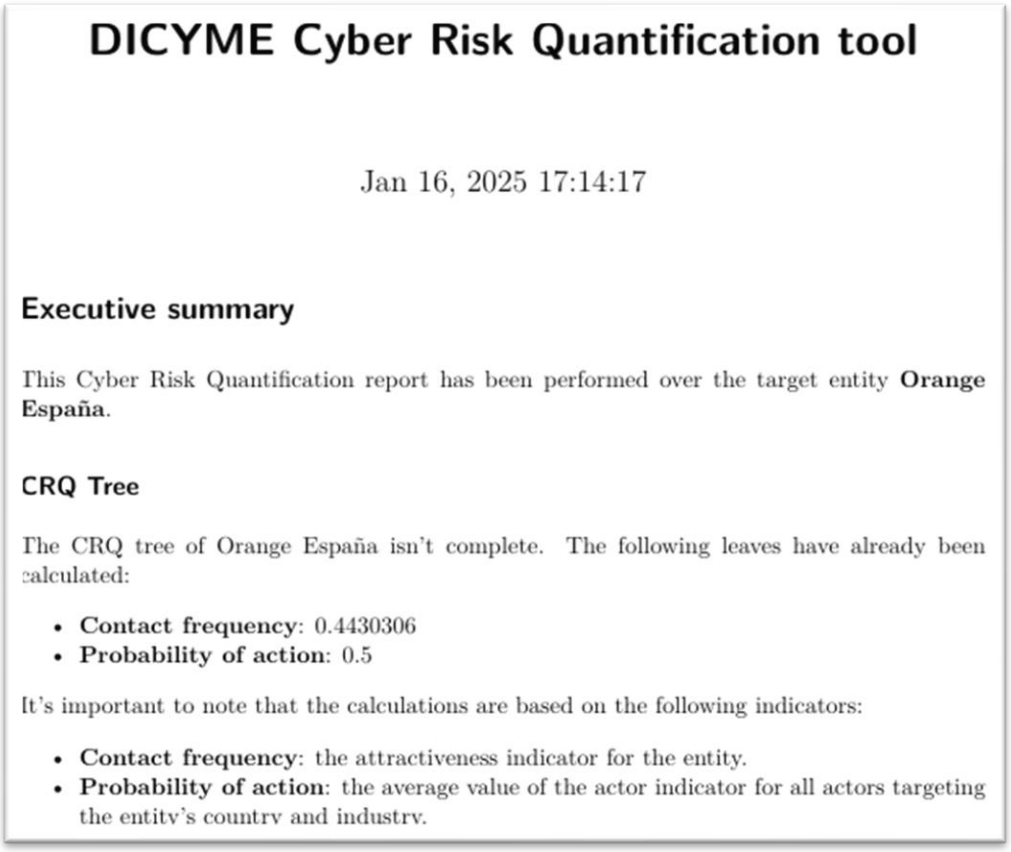
Ilustración 8. Idea conceptual para la estimación del impacto en una compañía

Al integrarse el módulo de estimación del ciber riesgo dentro de la aplicación web de DICYME, la infraestructura es la misma descrita en el entregable E3.1: la base de datos MongoDB en la que se almacenan los datos e indicadores del proyecto está alojada en servidores de la URJC, de igual manera que el Sistema. Está desarrollado principalmente en R, empleando Shiny, un *framework* gratuito y de código abierto para el desarrollo de aplicaciones web.

3.1 Generación de informe de resultados

Con el fin de soportar la toma de decisiones, alineado tanto con la actividad 3 como la 4 del proyecto, se ha incluido la generación de un informe dinámico que incluye los resultados de la estimación del ciberriesgo, como se muestra en el margen derecho de la Ilustración 5. Módulo de cálculo del ciberriesgo del Sistema. Este campo permite multitud de opciones y alternativas que se están explorando para futuros entregables, como la integración de información y datos de diferente índole en función del público objetivo (directivos, técnicos, aseguradoras), así como la inclusión de salidas o alternativas propuestas en el recomendador, pendiente de diseñar, diferentes idiomas, gráficos de la aplicación, etc.

Por el momento, se genera un informe en formato PDF (véase la Ilustración 9. Informe de resultados de prueba para Orange España.) que muestra las hojas del árbol previamente descritas, así como el método seguido para su cálculo. De esta manera, se puede compartir información de la aplicación en un formato estandarizado y altamente compatible para reflejar un resultado concreto, de forma que los diferentes actores involucrados en la toma de decisiones e implementación de acciones puedan acceder a él de manera sencilla.



DICYME Cyber Risk Quantification tool

Jan 16, 2025 17:14:17

Executive summary

This Cyber Risk Quantification report has been performed over the target entity **Orange España**.

CRQ Tree

The CRQ tree of Orange España isn't complete. The following leaves have already been calculated:

- **Contact frequency**: 0.4430306
- **Probability of action**: 0.5

It's important to note that the calculations are based on the following indicators:

- **Contact frequency**: the attractiveness indicator for the entity.
- **Probability of action**: the average value of the actor indicator for all actors targeting the entity's country and industry.

Ilustración 9. Informe de resultados de prueba para Orange España.

4 Informe de Resultados de Prueba

Se ha implementado una serie de pruebas unitarias en la aplicación web de DICYME con el objetivo de validar el código, asegurar su correcto funcionamiento y verificar que las funciones devuelven el tipo de datos esperado. Estas pruebas cubren los siguientes aspectos clave:

- Verificación de tipos de datos: Se verifica que las funciones devuelven el tipo de datos correctamente como puede ser una lista, un DataFrame, etc.
- Verificación de clase: Se valida que ciertas funciones devuelvan un objeto de una clase en específico como puede ser un gráfico.
- Manejo de avisos: Se comprueba que, en determinados casos, las funciones generen los avisos deseados.

A continuación, se muestra un ejemplo de prueba donde se verifica el tipo de datos devuelto por una función y se comprueba que se emita un aviso en un caso específico:

```
## Text ----
### get_title ----
expect_type(get_title("incidents_time_series"), "character")
expect_warning(get_title("unknown_place"), "Unknown place")
```

Estas pruebas se comprueban cada vez que se despliega una nueva versión, obteniendo un resultado como el de la siguiente figura:

```
== Results =====================================
Duration: 232.3 s

── Skipped tests (1) ──────────────────────────
• empty test (1): test-reports.R:1:1

[ FAIL 0 | WARN 0 | SKIP 1 | PASS 57 ]
```

5 Comentarios Finales

En este documento se abordan los primeros pasos introducidos en la aplicación web de DICYME para la estimación del ciber riesgo de una compañía. Concretamente, se detalla cómo se están empleando los módulos ATR2ATK y THRACT para estimar diferentes componentes del árbol de ciber riesgo basado en la metodología FAIR. Además, se aborda un concepto de la futura estimación del impacto empleando otros modelos de DICYME. No obstante, los equipos son conscientes de las limitaciones del enfoque actual y están trabajando para mejorar la propuesta y obtener el cálculo final del ciber riesgo, completando el resto de los nodos del árbol.

Además, se ha introducido una funcionalidad muy poderosa y versátil como es el informe de resultados generado en tiempo real, integrando las entradas del usuario y los resultados de los modelos.