

CRAS: APLICACIÓN SHINY PARA ANÁLISIS Y SIMULACIÓN DE RIESGOS DE CIBERSEGURIDAD

Emilio L. Cano, Carmen Lancho, Víctor Aceña, Marina
Cuesta, Rubén R. Fernández and Isaac Martín
Rey Juan Carlos University

CONTENIDO

- Motivación y contexto
- Funcionalidad: análisis de riesgos
- Implementación y despliegue
- Conclusiones

DISCLAIMER



MOTIVACIÓN

- Asignatura “Análisis y gestión de riesgos” en el grado en ciberseguridad de la URJC.
- Materiales heredados (“Legacy” powerpoints)
- Métodos cuantitativos explicados sin código
- La principal herramienta era un archivo excel con macros

CONTEXTO

- Grupo de investigación en fundamentos y aplicaciones de la Ciencia de Datos de la Universidad Rey Juan Carlos, DSLAB: <https://www.datasciencelab.es>
- Modelo FAIR: Factor Analysis of Information Risk, <https://www.fairinstitute.org>
- Herramienta OpenFair del Open Group

FUNCIONALIDAD: ANÁLISIS DE RIESGOS

HERRAMIENTA EXISTENTE

Open FAIR™ Risk Analysis



This tool lets analysts compare two risk states: the "current" (*status quo*) state and a "proposed" (mitigated) state. There are three pages, which may be navigated between using the buttons above. You may graph distributions of either Loss Events and Loss Magnitude.

Every box in white is an input. Analysts can start from the **Risk** page to set up the local currency and loss measure of annual loss exposure. On any page you may specify a percentile or a threshold of the output, and view the chance of exceedance.

Use the **Loss Event Frequency (LEF)** page to work at any level of the FAIR LEF tree to enter loss event-related data.

Use the **Loss Magnitude (LM)** page to enter Loss Magnitude data. You may also view either simulated Single Loss Magnitudes or Total Risk Exposure outcomes.

User's Guide

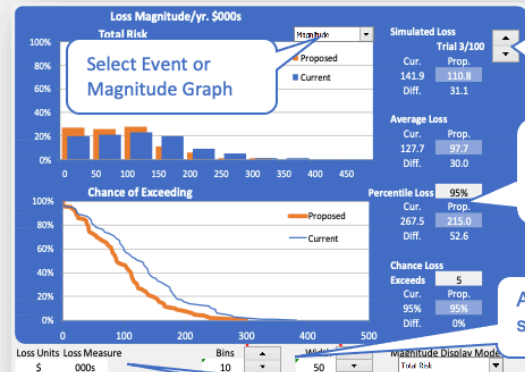


Probability Management



**SAN JOSÉ STATE
UNIVERSITY**

Risk



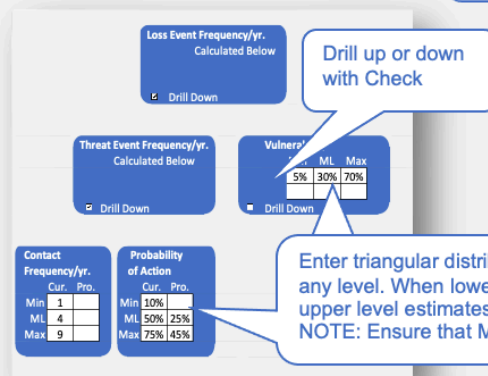
Scroll through individual simulation trials

Statistics based
on all trials
appear here

Adjust graph settings here

Set Units and Magnitudes
for all screens

Loss Event Frequency

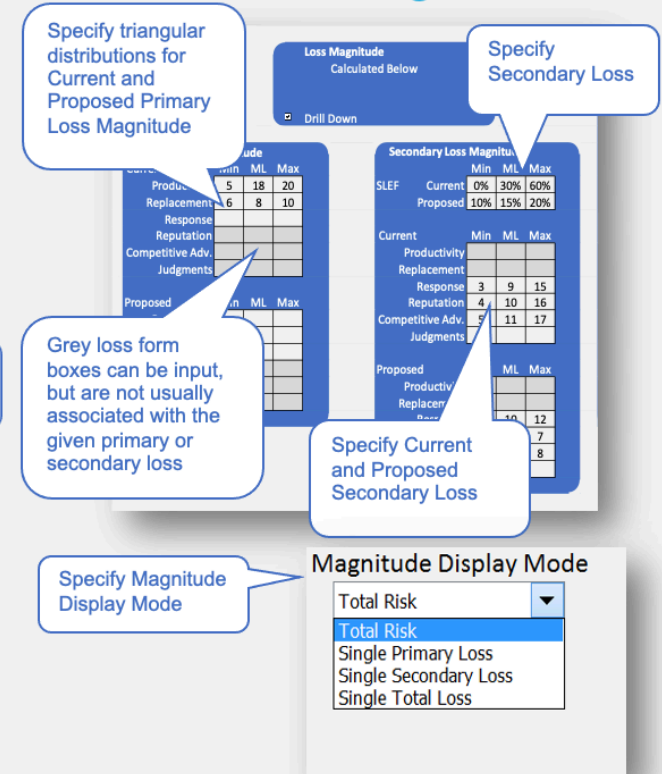


Enter triangular distributions estimates at any level. When lower levels are activated upper level estimates are bypassed.
NOTE: Ensure that $\text{Min} \leq \text{ML} \leq \text{Max}$.

Model created by Sam Savage, Danny O'Neil and Mike Jerbic with the
 SIPmath™ Modeler Tools from ProbabilityManagement.org
 HDR random number generator by Hubbard Decision Research
 Sums of IID triangular distributions from MetalogDistributions.com
 The Department of Economics at San Jose State University

[<Link>](#)
[<Link>](#)
[<Link>](#)
[<Link>](#)

Loss Magnitude



Specify triangular distributions for Current and Proposed Primary Loss Magnitude

Specify
Secondary Loss

Grey loss form boxes can be input, but are not usually associated with the given primary or secondary loss

Specify Current
and Proposed
Secondary Loss

Specify Magnitude Display Mode

Magnitude Display Mode


Total Risk	▼
Total Risk	
Single Primary Loss	
Single Secondary Loss	
Single Total Loss	

Copyright © 2018 The Open Group®. All Rights Reserved.
Open FAIR™ is a trademark of The Open Group.
SIPmath™ is a trademark of ProbabilityManagement.org.

APLICACIÓN SHINY CRAS

- Tres distribuciones de probabilidad (implementada una, exensible a más)
- Fijar semilla por reproducibilidad
- Paquete {bslib} para la estructura
- Descarga de datos simulados para usar con otras herramientas
- Flujo de trabajo más intuitivo

PÁGINA DE ENTRADA



Cybersecurity Risk Analysis and Simulation

OverviewParametersResultsData

<

Magnitude dist.

PERT

Event dist.

PERT

Simulation runs

#1000

Seed

🌱

e.g., 123

Instructions:

1. Select the probability distributions you are using to model loss event frequency and loss magnitude.

2. Change the number of simulations according to your preferences.

3. Set a seed if you want the results be reproducible.


4. Change the units of loss if needed (only for visualization purposes)

5. Go to the Parameters page. Input the values for the chosen probability distributions.

6. Run the simulations.

7. Go to the results page to visualize the results.

PARÁMETROS DE LAS SIMULACIONES



Cybersecurity Risk Analysis and Simulation

OverviewParametersResultsData

<

Magnitude dist.

PERT

Event dist.

PERT

Simulation runs

#100

Seed

e.g., 123

Run

Loss Magnitude

Min

0

Most Likely

50

Max

100

Proposed

New values:

0.0028.0063.00

Loss Event Frequency

Min

0

Most Likely

5

Max

10

Proposed

New values:

0.002.006.00

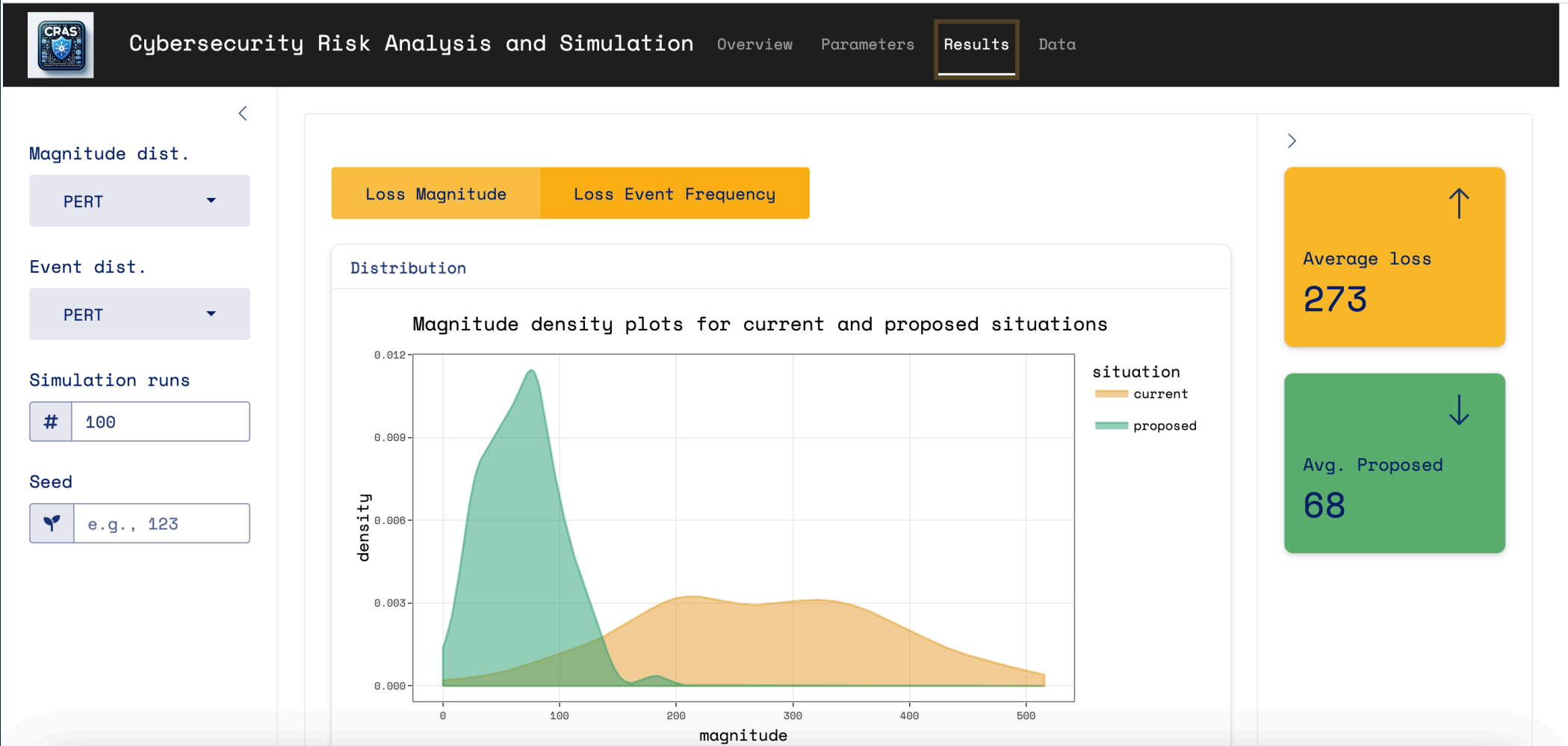
III Congreso y 14ª Jornadas de usuarios de R, Sevilla 2024-11-06

DSL³LAB
DATA SCIENCE LABORATORY

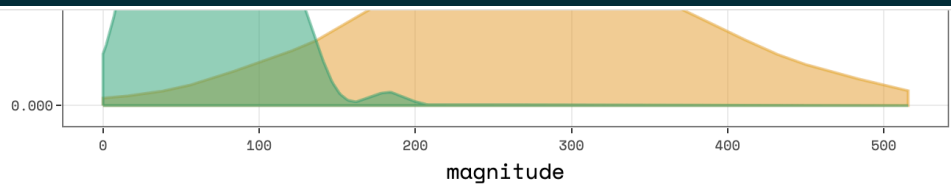
SIMULACIÓN

- Paquete {mc2d} para distribuciones PERT y triangular
- Implementando: beta y Log-normal
- Primer paso: se simulan los eventos en n años
- Segundo paso: se simula el gasto de cada evento

RESULTADOS

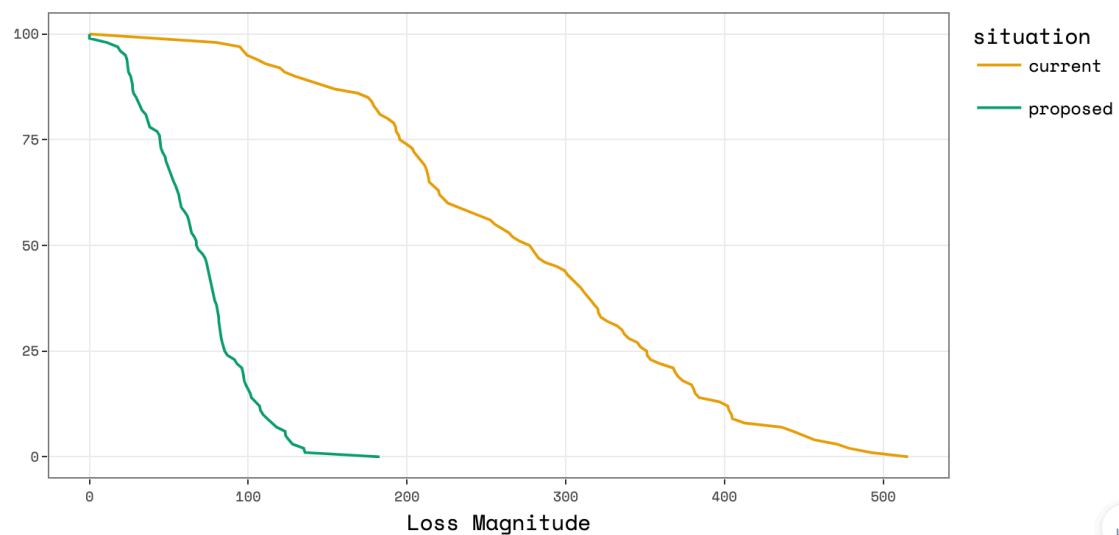


RESULTADOS




Chance of exceeding

Loss magnitude chance of exceeding



DATOS E INFORMES



Cybersecurity Risk Analysis and Simulation

OverviewParametersResultsData

Magnitude dist.

PERT

Event dist.

PERT

Simulation runs

#1000

Seed

e.g., 123

Show 10 entries

Search:

	situation	year	events	magnitude
1	current	1	5	226.98
2	current	2	5	258.619
3	current	3	4	142.631
4	current	4	4	189.518
5	current	5	7	331.132
6	current	6	6	262.076
7	current	7	5	197.682
8	current	8	6	193.874

0.0.0:3838/#tab-6134-4

IMPLEMENTACIÓN Y DESPLIEGUE

IMPLEMENTACIÓN

- Estructurado como un paquete (plantilla en [GitHub](#))
- Ventajas: documentación, pruebas unitarias, etc.
- Se ejecuta en el terminal (para desarrollo):

```
Rscript -e 'devtools::load_all();app_run()'
```

- En la consola:

```
cras::app_run()
```

- Repositorio: <https://github.com/URJCDSLAb/cras>

DESPLIEGUE

- Contenedor docker:

```
CMD ["R", "-e", "cras::app_run(.port =  
3804, .host = '0.0.0.0')"]
```

- En el servidor del DSLAB, junto con otras aplicaciones:
- <http://gondor.etsii.urjc.es:3804>

PROYECTOS DE INVESTIGACIÓN: DICYME

- Dynamic Industrial Cyber Risk Modelling based on Evidence (DICYME) research project (CPP2021-009025)
- Proyecto de colaboración público-privada con DeNexus TECH SL
- Dashboard: <https://gondor.etsii.urjc.es:3866>
- Conexión con MongoDB

CONCLUSIONES

RESULTADOS

- Enseñanza-aprendizaje de análisis de riesgos (con código R)
- Mejor comprensión de las distribuciones de probabilidad y simulaciones
- Reproducibilidad
- Exportación de datos e informes
- Gráficos interactivos

INVESTIGANDO

- Paquetes disponibles en el área
- Más distribuciones de probabilidad, calibración
- Otros dominios, por ejemplo riesgos operacionales en finanzas

TRABAJO FUTURO

- Implementar multilenguaje (véase <https://www.lcano.com/p/13jr/>)
- Incluir viñetas con documentación y métodos (con pkgdown)
- Completar la ontología FAIR
- Extender a otras metodologías y marcos de trabajo
- Integración continua
- Pruebas unitarias

GRACIAS!

<http://emilio.lcano.com>

emilio.lopez@urjc.es

Slides: emilio.lcano.com/p/14jres

Agradecimientos: Javier Sánchez García-Ochoa

Questions