Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 1
Sesión práctica 3:

Comparación entre CORAS y FAIR.

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. Comparación entre el modelo cualitativo CORAS y el modelo cuantitativo FAIR.

Examinar los resultados de ambos modelos puede resultar una tarea sumamente útil para evaluar la efectividad y exactitud en la detección y manejo de riesgos. Al comprobar que ambos modelos abordan los mismos riesgos, se facilita una comparación más detallada entre los resultados obtenidos en cada uno.

Por lo general, se espera que los resultados sean consistentes y que coincidan, lo que indicaría una alta fiabilidad en ambos modelos. Sin embargo, si los resultados no coinciden, es necesario realizar una revisión exhaustiva para determinar las posibles causas de esta discrepancia. Este proceso podría implicar examinar los datos de entrada empleados en cada modelo, evaluar la metodología utilizada en cada caso y considerar cualquier otra variable que pudiera haber influido en los resultados.

Para llevar a cabo una comparación entre ambos modelos, es necesario convertir el modelo CORAS en algo cuantitativo. Por ende, asignaremos valores numéricos a la probabilidad de que ocurra un evento, facilitando así el análisis comparativo.

VALOR CORAS (cualitativo)	Raramente	En ocasiones	Regularmente	Frecuentemente
VALOR CORAS (cuantitativo)	0% - 20%	21% - 50%	51% - 80%	81% - 100%

Una vez hemos obtenido la tabla con la conversión a valores cuantitativos, compararemos los dos resultados en base a los riesgos:

- **Brecha de datos que afecta al código de la aplicación:** Teniendo en cuenta el modelo FAIR, este nos indica que la probabilidad de ocurrencia de este riesgo en un año es del *46%*, mientras que, CORAS, nos indica que *Raramente* podría ocurrir. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

- **Ransomware:** Teniendo en cuenta el modelo FAIR, este nos indica que la probabilidad de ocurrencia de este riesgo en un año es del 93%, mientras que, CORAS, nos indica que *en ocasiones* podría ocurrir. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

- **Brecha de datos que afecta al cliente:** Teniendo en cuenta el modelo FAIR, este nos indica que la probabilidad de ocurrencia de este riesgo en un año es del 97%, mientras que, CORAS, nos indica que *regularmente* podría ocurrir. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

- **Denegación de servicio:** Teniendo en cuenta el modelo FAIR, este nos indica que la probabilidad de ocurrencia de este riesgo en un año es del 92%, mientras que, CORAS, nos indica que *regularmente* podría ocurrir. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

Tras examinar los resultados obtenidos, comprobamos que no existe coincidencia alguna entre los dos modelos. Esto se puede dar debido a lo siguiente:

- **Brecha de datos que afecta al código de la aplicación:** Calificamos este riesgo de acuerdo con el enfoque CORAS como raramente, dado que percibimos que la capacidad de amenaza es variable, influenciada por la habilidad y recursos del posible adversario. Además, al ser una start-up, no estimamos que haya una alta demanda de personas interesadas en el código de la aplicación.

  No obstante, en el enfoque de FAIR, se exploró con mayor detalle el uso de dispositivos portátiles y servicios de terceros, junto con la política de seguridad de contraseñas relativamente permisiva de ChaseMyCash.

- **Ransomware:** De acuerdo con FAIR este porcentaje se estableció en un 93% debido a la falta de medidas de seguridad para contrarrestar este tipo de ataques, como la utilización de dispositivos móviles no corporativos. En contraste, CORAS se centró más en la probabilidad de que los dispositivos estén infectados con malware preinstalado, provocando que este porcentaje sea menor.

- **Brecha de datos que afecta al cliente:** Aunque los dos métodos presentan una discrepancia notable, esta disparidad no es tan significativa como la observada en los apartados anteriores. Nuestra evaluación de la probabilidad de ocurrencia, basada en el enfoque FAIR, sugiere un 97% de probabilidad, considerando diversas amenazas potenciales como la filtración de datos confidenciales de clientes por parte de empleados, el robo de credenciales de empleados o la explotación de vulnerabilidades en la red o la aplicación. Por otro lado, en CORAS se hace hincapié en el acceso no autorizado una vez que este ha ocurrido.

- **Denegación de servicio:** Finalmente, de acuerdo con el análisis basado en FAIR, se ha determinado una probabilidad del 92%, considerando diversos factores como la visibilidad de la empresa, la naturaleza de su actividad y la presencia de un adversario motivado para llevar a cabo dicho ataque. En cuanto al enfoque CORAS, se ha calificado como *regularmente*, dado el uso de infraestructura AWS, específicamente AWS VPC, lo cual ha reducido significativamente su probabilidad.

Por otra parte, hay que tener en cuenta las pérdidas que se producen según los modelos, por ello, convertiremos en cuantitativas las pérdidas económicas.

VALOR CORAS (cualitativo)	Leve	Moderado	Grave	Catastrófico
VALOR CORAS (cuantitativo)	0€ - 70.000€	70.001€ - 135.000€	135.001€ - 290.000€	+290.001€

- **Brecha de datos que afecta al código de la aplicación:** Teniendo en cuenta el modelo FAIR, este nos indica que el impacto económico de este riesgo en un año es de *110.000*€, mientras que, CORAS, nos indica que el impacto es *GRAVE*. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

- **Ransomware:** Teniendo en cuenta el modelo FAIR, este nos indica que el impacto económico de este riesgo en un año es de *149.000*€, mientras que, CORAS, nos indica que el impacto es *GRAVE*. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

- **Brecha de datos que afecta al cliente:** Teniendo en cuenta el modelo FAIR, este nos indica que el impacto económico de este riesgo en un año es de *606.300*€, mientras que, CORAS, nos indica que el impacto es *CATASTRÓFICO*. Conociendo esto podemos concluir que ambos modelos coinciden.

- **Denegación de servicio:** Por último, respecto el modelo FAIR, este nos indica que el impacto económico de este riesgo en un año es de *455.500*€, mientras que, CORAS, nos indica que el impacto es *GRAVE*. Conociendo esto podemos concluir que existe una discrepancia entre los dos métodos.

2. Conclusiones del proceso de análisis.

2.1 Riesgo de brecha de datos que afecta al código de la aplicación.

Se ha de destacar que ambos enfoques produjeron resultados distintos debido a sus metodologías particulares. A pesar de estas discrepancias, se reconoció la importancia de tener en cuenta este aspecto al evaluar las posibles pérdidas de la empresa, dado que ambas metodologías analizaron la misma situación. Por ello, se concluye que, a pesar de las diferencias metodológicas, ambos enfoques proporcionan resultados importantes que deben ser considerados en la gestión del riesgo empresarial.

2.2 Riesgo de ransomware.

Los resultados obtenidos, al igual que con el riesgo de brecha de datos que afecta al código de la aplicación, mostraron una disparidad total. Esta discrepancia se debe a la adopción de enfoques distintos en ambas metodologías, similar a lo observado con el riesgo mencionado anteriormente.

En términos económicos, también se observó una disparidad clara entre los métodos, aunque en este caso la diferencia no fue tan marcada como en la probabilidad de riesgo. Esto se debe a que el costo de mitigar un ataque o proteger los sistemas es comparativamente similar en ambos enfoques.

2.3 Brecha de datos que afecta al cliente.

Utilizando el método CORAS, se ha identificado que la brecha de datos se sitúa en la categoría de alto riesgo en la matriz de riesgos, indicando que es un riesgo de ocurrencia frecuente con un impacto catastrófico. Esto se debe a la diversidad de amenazas que pueden desencadenar una brecha de datos, lo que sugiere que la probabilidad de que ocurra es prácticamente del 100%. En otras palabras, es altamente probable que se experimente al menos una instancia de este tipo cada año.

Además, es crucial resaltar que las repercusiones económicas asociadas a este riesgo son considerablemente altas y pueden tener efectos graves en la organización. Por consiguiente, es esencial tomar medidas proactivas para mitigar el riesgo lo más pronto posible y reducir sus impactos en caso de materializarse. Se debe prestar una atención especial a la seguridad de los datos y garantizar su protección adecuada para evitar posibles brechas.

2.4 Denegación de servicio.

Por último, y de manera similar al riesgo de la brecha de datos que impacta al cliente, la probabilidad de que ocurra este evento es prácticamente segura. Las diferencias se encuentran en que la metodología CORAS ha tenido en cuenta las tecnologías ya implementadas por la empresa, como los sistemas AWS, los cuales, gracias a sus controles internos, pueden mitigar ciertos ataques de este tipo. Sin embargo, en FAIR esta variable no fue considerada, ya que simplemente se calculó la probabilidad de que ocurra el evento sin tener en cuenta esta tecnología concreta. Dado que este tipo de ataque es uno de los más comunes empleados por los ciberdelincuentes, la probabilidad de ocurrencia según esta metodología se situó en alrededor del 90%.

De este modo, según la metodología FAIR, que considera una probabilidad de ocurrencia más alta, la pérdida económica también ha sido mayor. Mientras tanto, la metodología CORAS, que contempla una probabilidad menor, ha resultado en una pérdida económica también menor.

3. Propuesta de mejoras y limitantes.

En cuanto a CORAS, una limitación evidente es su falta de consideración explícita del impacto económico o financiero derivado de las amenazas identificadas. Como resultado, en ocasiones esta metodología podría subestimar el verdadero costo de una amenaza.

Por otro lado, aunque la metodología FAIR es más exhaustiva en términos de evaluar el impacto económico de las amenazas y riesgos, su principal desventaja radica en que requiere una gran cantidad de datos y experiencia. Esto puede hacer que sea costosa y compleja de implementar para algunas organizaciones.

Como área de mejora para CORAS, sería beneficioso incluir una evaluación más detallada de las amenazas emergentes y nuevas tecnologías, especialmente en el ámbito de la seguridad de la información. Esto permitiría a las organizaciones anticiparse a posibles amenazas futuras y tomar medidas preventivas antes de que se materialicen.

En cuanto a FAIR, una mejora potencial sería simplificar la metodología y reducir la complejidad de los modelos utilizados. Esto haría que la metodología fuera más accesible para aquellas organizaciones con recursos limitados y sin personal especializado en análisis de riesgos.