Ingeniería de la Ciberseguridad
Curso 2023/2024

Sesión práctica 1:

Informe ejecutivo. FAIR

Análisis y Gestión del Riesgo

Realizado por:

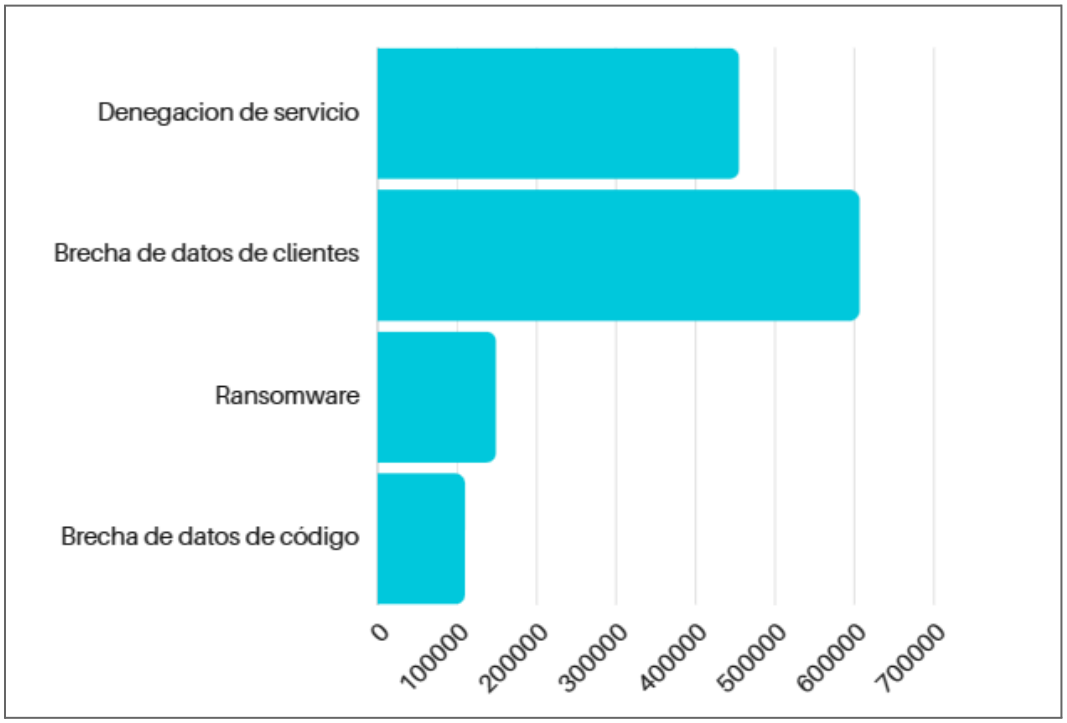
Gabriel Izquierdo González

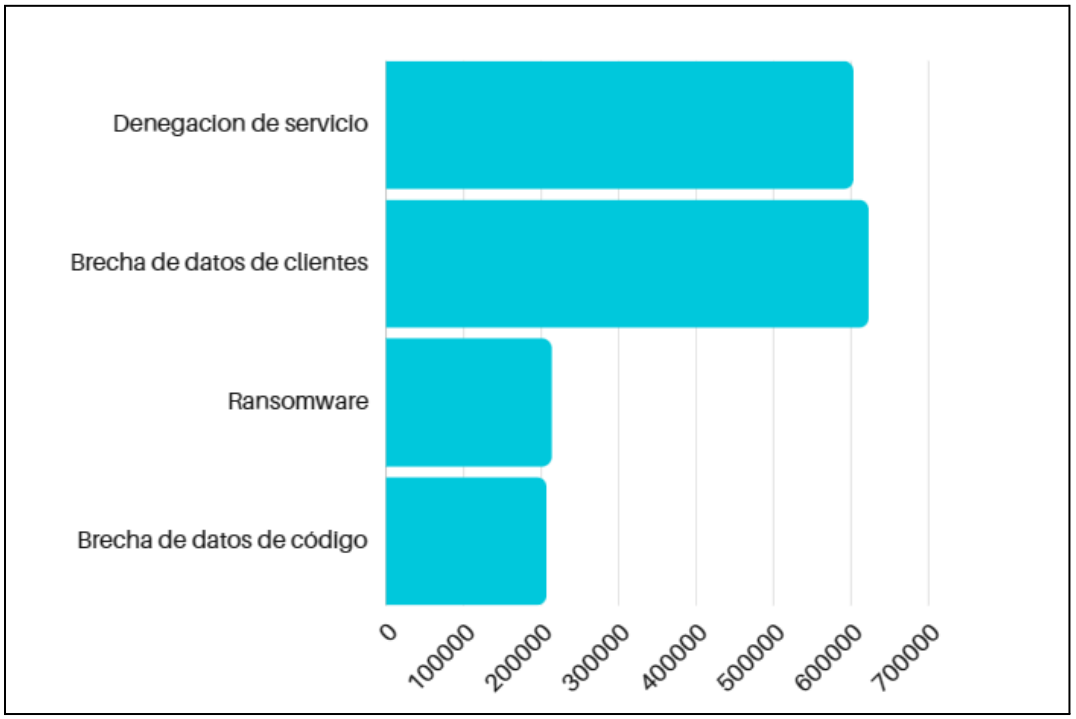
Mario Ruano Diaz

Juan Antonio Suárez Suárez

1. Informe

En la siguiente gráfica se presentan las pérdidas totales proyectadas para la empresa debido a cada uno de estos riesgos, tanto antes como después de la implementación de las mejoras:





2. Mejora en el riesgo de brecha de datos que afecta al código.

En esta sección, se llevarán a cabo mejoras en los métodos de análisis de riesgos utilizados.

En relación a CORAS, una mejora potencial sería considerar que los correos electrónicos de los empleados anteriores se redirijan a su sucesor. Esto podría evitar que un ex-empleado mantenga acceso al repositorio de código, lo que podría resultar en filtraciones o modificaciones no autorizadas.

En cuanto a FAIR, la modificación se centrará en la probabilidad de acción. En este caso, la probabilidad de acción, que tenía un valor medio de 0.25 para este riesgo, será reemplazada por un valor que calcularemos utilizando el teorema de Bayes.

Vamos a calcular la probabilidad de acción como la posibilidad de que ocurra una brecha de datos que afecte al código, sabiendo que ya ha ocurrido una brecha de datos en general. Para esto, utilizaremos la siguiente fórmula.

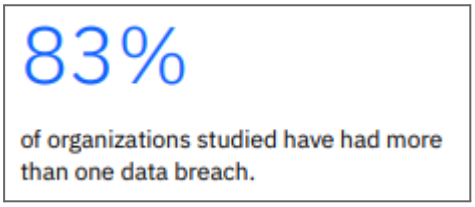
P(A|B) = P(A) · P(B|A) / P(B)

En este caso, P(A) será la probabilidad de que se produzca una brecha de datos en el código. Por otra parte, P(B) será la probabilidad de que se haya producido una brecha de datos.

Según el siguiente informe de la empresa "Synopsys", se detectó al menos una vulnerabilidad crítica en el 48% de las bases de datos analizadas. Este será nuestro P(A).

> Además, los investigadores de Synopsys también descubrieron que había vulnerabilidades de alto riesgo en el 48% de las bases de código que analizaron. Estas vulnerabilidades han sido explotadas activamente, ya cuentan con pruebas de concepto documentadas o están clasificadas como vulnerabilidades de ejecución remota de código.

El valor de P(B) se asignará según el siguiente reporte de IBM:

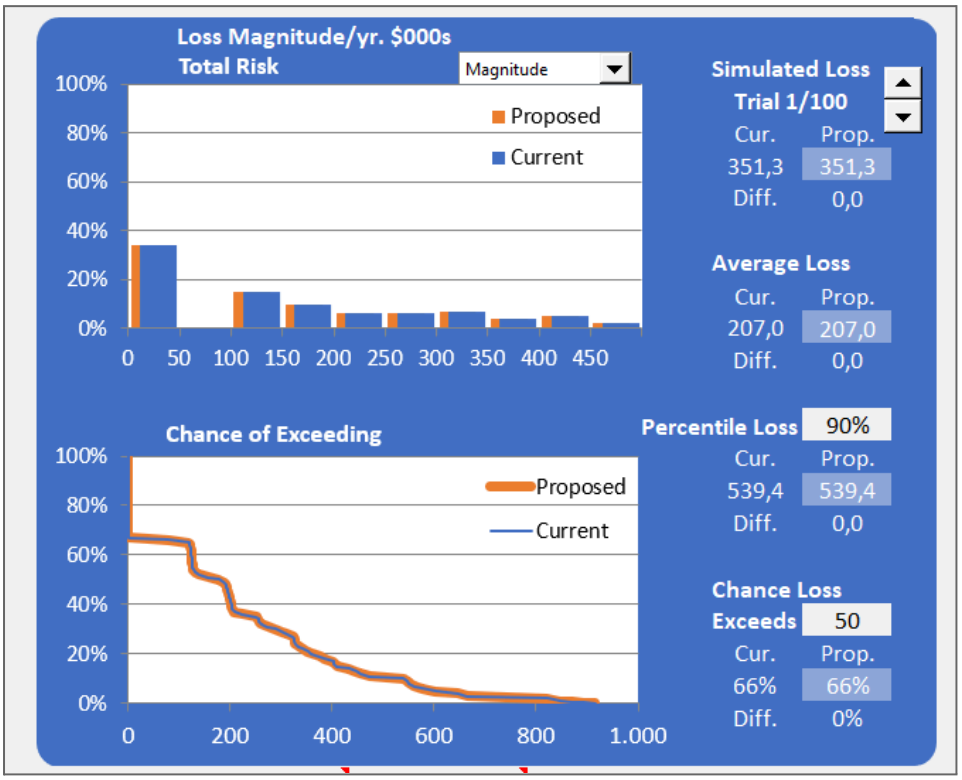


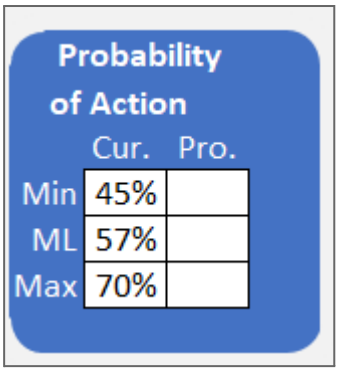
Por lo tanto;

P(A|B) = P(A) · P(B|A) / P(B)

P(A|B) = 1 * 0,48 / 0.83 = 0.57

Conociendo este dato, establecemos el valor alto en 70% y el valor bajo en 45%.





Después de implementar las mejoras, las pérdidas anuales para la brecha de datos que afecta al código han aumentado de 110,000€ a 207,000€. Este cambio representa una alteración muy notable en el panorama económico, prácticamente del doble.

3. Mejoras en el riesgo de ransomware

En este apartado, se llevarán a cabo mejoras en los métodos de análisis de riesgos utilizados.

En relación con CORAS, una mejora potencial sería considerar no solo el uso de dispositivos personales en lugar de corporativos, sino también todas las implicaciones asociadas.

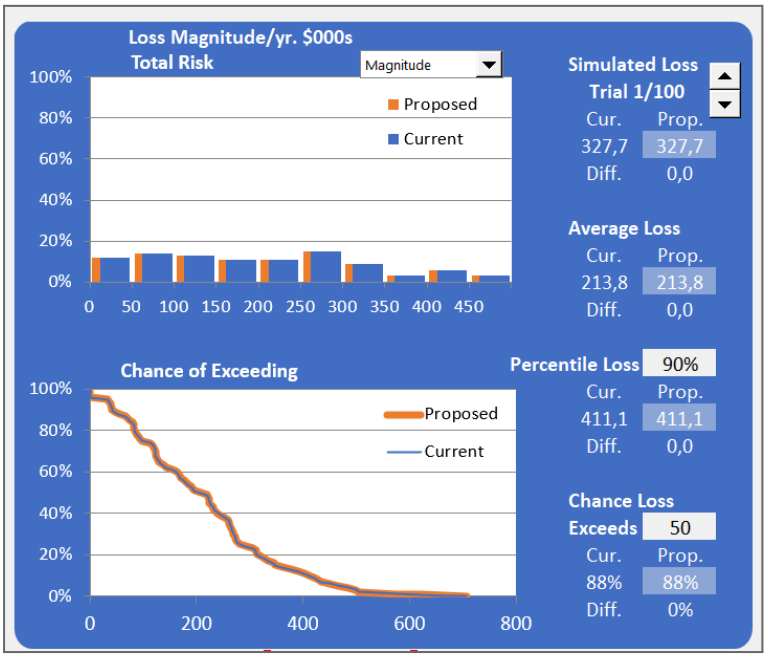
Estos dispositivos suelen carecer de suficiente protección, lo que aumenta las probabilidades de que los ciberdelincuentes realicen ataques de phishing o de que los propios empleados descarguen aplicaciones de terceros no confiables, lo que puede resultar en la infección del dispositivo y poner en riesgo a la empresa.

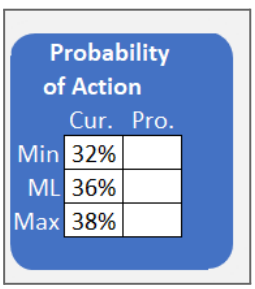
Por otra parte, otra mejora en CORAS sería ajustar la probabilidad de ocurrencia, que actualmente se define como "en ocasiones", mientras que en FAIR se obtuvo una media de 2 eventos de este tipo al año. Como mejora, se ha decidido establecer la métrica en "regularmente".

En cuanto a FAIR, según el informe de Sophos sobre el ransomware en 2023, se realizó un estudio en un total de 3000 empresas, de las cuales el 66% (1980 empresas) fueron afectadas por ransomware. Por lo tanto, 1020 empresas no sufrieron ataques de este tipo.

Conociendo esto: α = 1980, β = 1020.

<u>Valor mínimo:</u> 31,53%
<u>Valor medio:</u> 35,85%
<u>Valor máximo:</u> 38,42%





Después de implementar las mejoras, las pérdidas anuales para el ransomware han aumentado de 149,200€ a 213,800€. De la misma manera, este cambio representa una alteración muy notable.

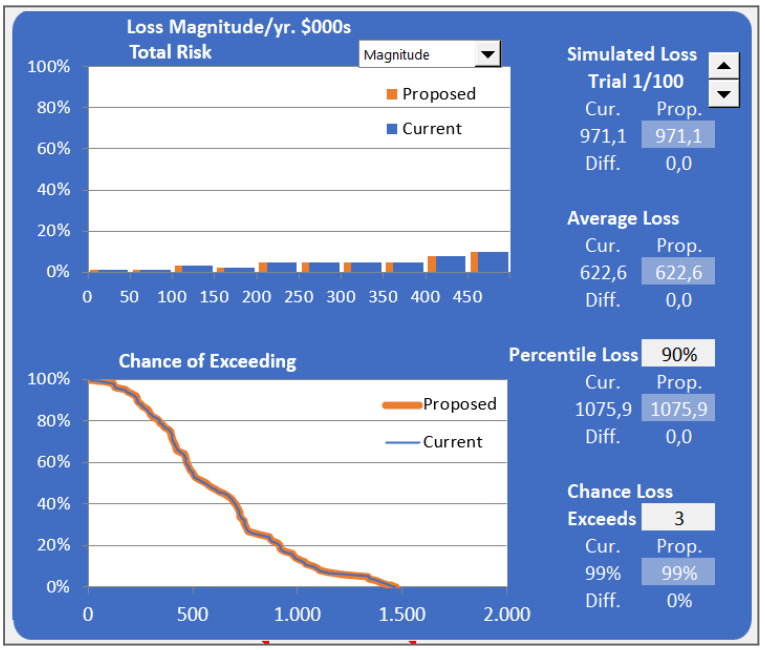
4. Mejoras en el riesgo de brecha de datos de clientes

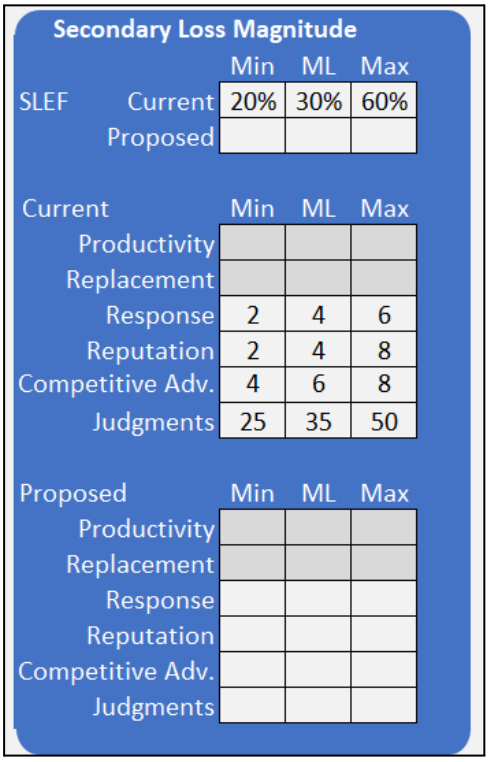
En este apartado se llevarán a cabo mejoras en los métodos de análisis de riesgos utilizados. Es importante destacar que, tras comparar las metodologías, ambos informes de riesgos muestran una notable similitud, lo que sugiere que el estudio es bastante acotado.

En relación con CORAS, una posible mejora sería considerar no solo la amenaza de un atacante externo (hacker), sino también la posibilidad de amenazas internas provenientes de los propios empleados de la organización. Dado que estos empleados tienen todos los privilegios de administración, podrían acceder completamente a la base de datos y extraer información sensible. Este riesgo puede surgir de un empleado insatisfecho con su entorno laboral, salario, reconocimiento, oportunidades de ascenso, trato de los superiores o compañeros, quién podría sentirse resentido y decidir atacar a la empresa como forma de venganza o protesta.

Por otro lado, en cuanto a FAIR, es importante tener en cuenta que la exposición de estos datos personales puede dar lugar a sanciones por parte de la AEPD (Agencia Española de Protección de Datos) debido a una protección inadecuada de los mismos. Según lo establecido en la LOPD-GDD, las sanciones pueden alcanzar hasta veinte millones de euros o el 4% del volumen de negocio anual, dependiendo de la gravedad de la infracción cometida.

Se calcularán los costes derivados como el 4% del volumen de negocio anual, dado que no se facturan 20 millones anualmente.





El cambio es relativamente insignificante, ya que el incidente aún costaría un promedio de 622,600€ al año. Esto confirma que el análisis inicial estaba correctamente delimitado.

5. Mejoras en el riesgo de denegación de servicio

Como se ha procedido a hacer en los casos anteriores, se han revisado los resultados para considerar si hay áreas de mejora tanto en la metodología CORAS como en la metodología FAIR, en este caso en cuanto al riesgo de interrupción de servicio, con el objetivo de conseguir resultados más precisos.

En cuanto al riesgo de interrupción de servicio se han identificado tres posibles mejoras para la metodología CORAS:

En primer lugar, al tratarse de una metodología más cualitativa no era sencillo establecer valores precisos para la escala de probabilidades generalizada que se presentó para los 4 riesgos, algo de lo que nos hemos percatado cuando se utilizó posteriormente una metodología más cuantitativa, como es la de FAIR . En concreto, consideramos que esta escala de probabilidades debería ser revisada, asignando al campo "frecuentemente" (el mínimo), un valor "ocurre como máximo una vez cada 1 mes", ya que tiene el valor de cada 3 meses. Hemos considerado que esto sería lo más adecuado, porque específicamente, en el caso de este riesgo, al ser evaluado con la metodología FAIR, se obtuvieron resultados de 16 ataques de este tipo al año (es decir, uno cada 22 días y medio).

En segundo lugar, al establecer un incidente no deseado para este riesgo, se decidió escoger una eliminación accidental de la información de la base de datos, algo que tiene una probabilidad de ocurrencia muy baja para ataques de tipo interrupción de servicio y no representa en su totalidad a estos, pudiendo ser más común seleccionar un ataque de inundación de paquetes (ataque que implica el envío de un gran volumen de tráfico de red a la víctima, lo que satura el ancho de banda y dificulta el acceso a los recursos de la red).

Como última mejora para este riesgo en cuanto a CORAS, se propuso una escala de impacto que se centraba en los daños en términos de beneficios perdidos y el tiempo de inactividad. Para conseguir resultados más concisos se podría añadir a esta escala la valoración de otros factores como el volumen de tráfico generado y el tipo de ataques de interrupción de servicio, ya que ambos pueden proporcionar información valiosa y más detallada sobre la gravedad del ataque y su capacidad para afectar la red y el negocio en general.

A continuación, nos centraremos en la mejora de la metodología FAIR, la cual fue elaborada de la forma más minuciosa, detallada y profunda, por lo cual es difícil introducir alguna mejora.

Según un artículo de B2B y Kaspersky, un 38% de las empresas confirma haberse enfrentado a al menos un ataque de DDoS.

> Según los datos del informe elaborado por B2B Internacional y **Kaspersky Lab**, el 38 por ciento de las empresas que prestan **servicios online**, tales como compras, medios de comunicación y otros similares, fue víctima de **ataques DDoS** en los últimos 12 meses.

La encuesta se realizó a un total de 3900 entidades, por lo que, el número de empresas afectadas por el ataque de denegación de servicio fue de 1482, y 2416 no se vieron afectadas. Siguiendo la distribución alfa-beta:

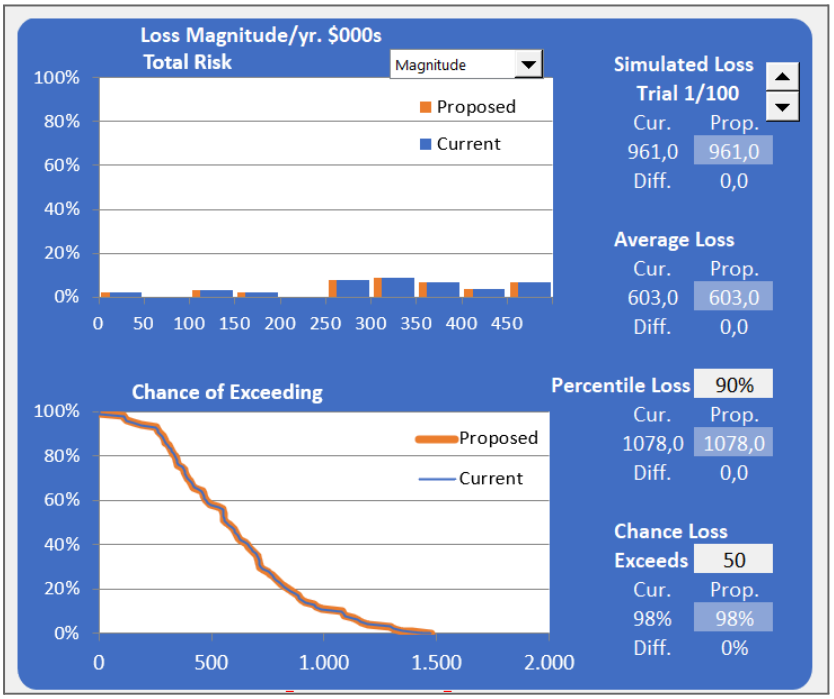
α = 1482, β = 2416 .

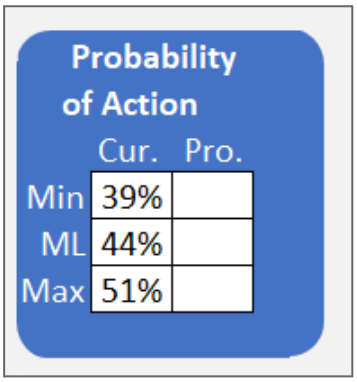
Valor mínimo: 39,55%

Valor medio: 44,00%

Valor máximo: 51,39%

> A total of 3,900 respondents from 27 countries – including representatives from companies of all sizes – took part in this year's survey. The survey was bigger than last year's, both in total





Después de implementar las mejoras, las pérdidas anuales para la denegación de servicio han aumentado de 455,500€ a 603,000€. De nuevo, este cambio representa una alteración notable.