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

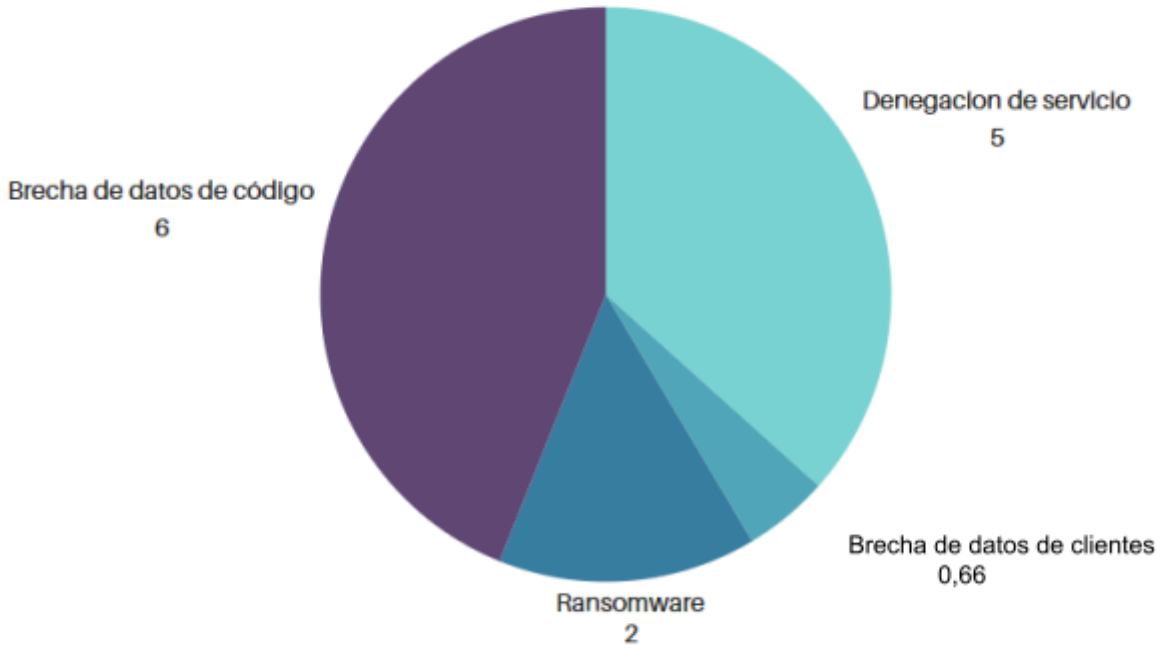
El propósito de este informe es realizar una evaluación completa sobre el nivel de riesgo relacionado con los problemas más recurrentes y críticos en la empresa ChaseMyCash. Para ello, llevaremos a cabo un análisis minucioso de estos problemas, con el objetivo de identificar sus causas y consecuencias principales.

Análisis.

Para llevar a cabo el análisis de riesgos, se ha empleado la metodología *FAIR*, la cual se enfoca en la identificación de activos de información críticos y en el análisis de los riesgos vinculados a estos activos. Esto capacita a las organizaciones para tomar decisiones fundamentadas sobre cómo mitigar o transferir estos riesgos.

Mediante esta metodología, se ha desarrollado un modelo para los cuatro riesgos identificados, el cual calcula *la frecuencia de contacto anual* que muestra la probabilidad de que una amenaza realmente entre en contacto con el recurso, *la probabilidad de acción*, que determina la probabilidad de que la amenaza actúe una vez que haya entrado en contacto con el recurso, *la capacidad de amenaza*, que indica el nivel de fuerza que la amenaza puede aplicar sobre el recurso, y por último, *la fuerza de resistencia*, que indica la capacidad del recurso para resistir la amenaza.

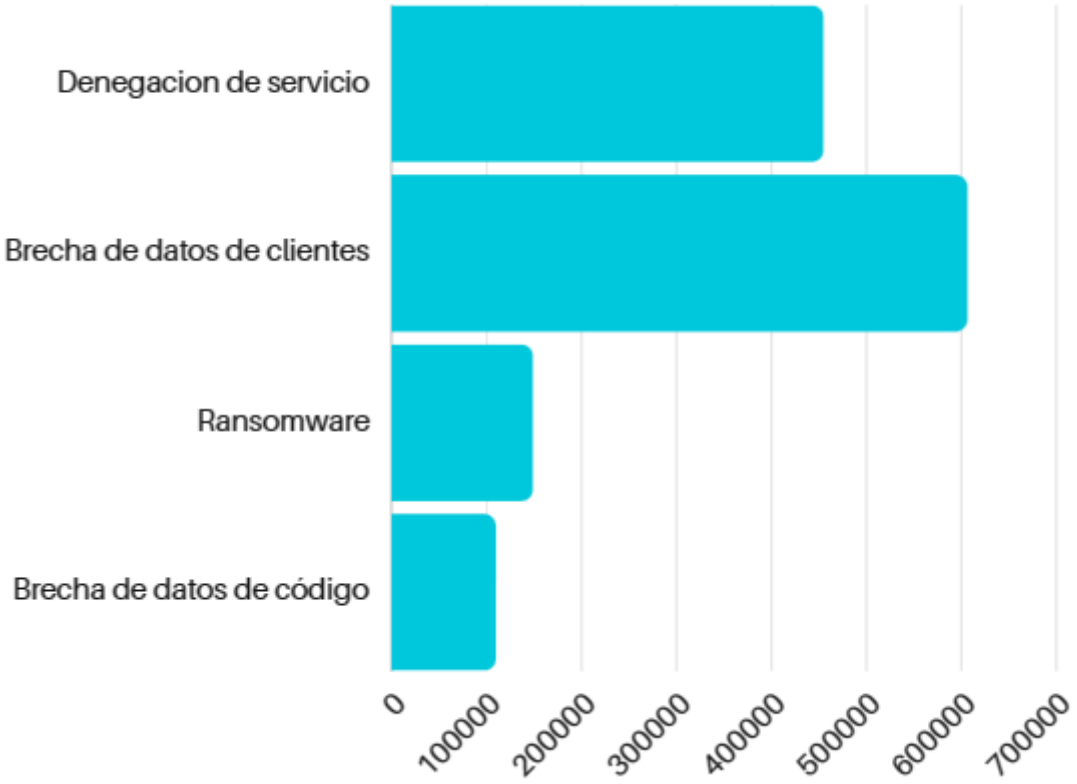
Seguidamente, hemos llevado a cabo un análisis de la probabilidad de ocurrencia, a partir del cual hemos llegado a las siguientes conclusiones sobre la frecuencia esperada de ataques que se producirán anualmente para cada uno de los cuatro tipos de riesgos identificados.



Impacto.

En este apartado, nos enfocaremos en calcular tanto las pérdidas primarias, las cuales abarcan la pérdida de productividad, los costos de reemplazo y respuesta, como las pérdidas secundarias, que incluyen la probabilidad de pérdidas adicionales, los costos de respuesta, la pérdida de reputación, la pérdida de ventaja competitiva y los potenciales litigios que la empresa podría enfrentar en tal situación.

Conociendo esto, el siguiente gráfico muestra las pérdidas anuales que podrían presentar en el caso de que se produjeran dichos incidentes asociados a los 4 riesgos:



Estos riesgos deben ser abordados con prontitud para minimizar su efecto en la privacidad y seguridad de los clientes, así como en la reputación de la empresa. La brecha de datos de código es el único riesgo que puede ser tolerado, lo que significa que la empresa puede implementar medidas para mitigarlo, aunque no es necesario hacerlo de manera inmediata ya que puede ser gestionado sin generar un gran impacto negativo en la empresa.