Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 1
Sesión práctica 2:

FAIR.

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. SEGURIDAD CORPORATIVA

1.1 RANSOMWARE

Objetivo

El objetivo es estimar la probabilidad e impacto asociados que tendrá nuestra empresa ChaseMyCash en caso de que un ransomware se propague por nuestra empresa debido a un acceso no autorizado, por un dispositivo externo a la empresa o bien por culpa de algún empleado.

Contexto

Visto que la empresa ChaseMyCash no proporciona móviles corporativos y se permite a los empleados el uso de sus propios teléfonos móviles para trabajar nos deja ver un posible vector de entrada de amenazas para la compañía ya que los teléfonos móviles personales no están configurados con las medidas de seguridad requeridas por la empresa. Además, al no ser un dispositivo de la empresa, esta no tendrá el control total sobre el mismo para poder proteger la posible información confidencial y sensible perteneciente a la empresa.

Activos

Los posibles activos en riesgo serán tanto los dispositivos personales de los empleados como todo lo relacionado con el código de la aplicación, la información sensible de la empresa que tenga almacenada en el teléfono personal y la reputación corporativa.

Adversario

Los posibles adversarios podrían ser tanto atacantes solitarios como grupos de ciberdelincuentes que buscan beneficio económico pidiendo rescate, dañar la imagen de la empresa o simplemente destruir datos.

Tipo de amenaza

El ransomware se clasifica como una amenaza perjudicial y deliberada, ya que tiene como objetivo obtener ganancias económicas mediante la extorsión a la víctima. El perpetrador suele emplear tácticas como el correo electrónico fraudulento o la explotación de vulnerabilidades en la infraestructura de red de la empresa para introducir el software malicioso y encriptar los archivos.

Impacto amenaza

Un ataque de ransomware puede incidir en múltiples aspectos fundamentales de la ciberseguridad. En primer lugar, la accesibilidad de los datos de la empresa se ve gravemente comprometida, dado que los archivos encriptados quedan inaccesibles para el personal. Además, la confidencialidad de la información sensible de los usuarios se ve comprometida, puesto que los atacantes pueden acceder a los datos cifrados. Por último, la integridad de los datos corre peligro si los archivos encriptados no pueden ser recuperados o si los atacantes optan por filtrarlos o eliminarlos. En general, un ataque de ransomware puede generar repercusiones económicas, operativas y de reputación significativas para la empresa afectada.

Alcance

Datos de ChaseMyCash se refiere a tanto código de la aplicación como a la información sensible.

Activo en riesgo	Adversario	Tipos de Amenaza	Impacto de la amenaza
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Integridad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad
Dispositivos y servicios ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad

Análisis

- ### Frecuencia de contacto.

  En este caso, la frecuencia de contacto se define como la cantidad de horas que los empleados utilizan sus dispositivos personales para acceder a servicios o sistemas internos de ChaseMyCash. Esta evaluación se ha llevado a cabo mediante una serie de cuestionarios dirigidos a todos los empleados, donde se especifica que, durante un año laboral típico, los dispositivos personales se

utilizan durante aproximadamente 1000 horas (equivalentes a 41,66 días). Basándose en esta medida, se establece un mínimo de 500 horas al año (equivalente a 20,83 días) y un máximo de 1500 horas al año (equivalente a 62,5 días).

- **Probabilidad de acción.**

  La "probabilidad de acción" se define como la posibilidad de que un empleado cometa un error de seguridad que resulte en la propagación de malware dentro de la empresa. Dado que ChaseMyCash no ofrece dispositivos con configuración empresarial, es probable que muchos de los dispositivos utilizados por los empleados carezcan de las medidas de seguridad adecuadas, como la falta de software antivirus. Es altamente probable que los requisitos mínimos de seguridad necesarios para proteger los datos tanto de la empresa como de sus clientes no se cumplan. Por lo tanto, se establece que el porcentaje mínimo de esta probabilidad sea del 15%, con un promedio del 25% y un máximo del 35%.

- **Capacidad de amenaza**

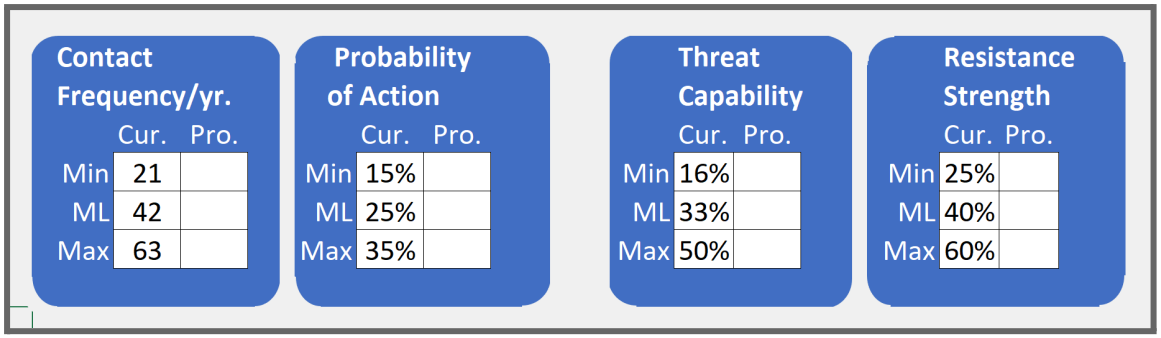
  Dado que estamos estimando la probabilidad y el impacto asociado a un ransomware nos basaremos en las estadísticas oficiales de Sophos de 2023. 50% (Percentage of Organizations Hit by Ransomware In the Last Year). Vamos a establecer este valor como el máximo, siendo el promedio 33% y el mínimo 16%.

- **Fuerza Resistencia**

  La "fuerza de resistencia" se ve influenciada por varios factores. A pesar de la falta de medidas de seguridad implementadas por parte de ChaseMyCash, existe un aspecto positivo relacionado con su uso de servicios en la nube. La propagación del ransomware a través de la red interna de una organización puede ser más lenta en comparación con los servicios en la nube. Esto se debe a que los servicios en la nube suelen contar con medidas de seguridad más avanzadas, como firewalls, monitoreo de red y análisis de comportamiento, que pueden detectar y bloquear el ransomware de manera más efectiva que las redes internas. Es importante tener en cuenta esta ventaja al evaluar la capacidad de resistencia de la empresa ante posibles ataques de ransomware.

  Por lo tanto los valores definidos son: el máximo 60%, el promedio 40% y el mínimo 25%.

Resumen de los valores utilizados:



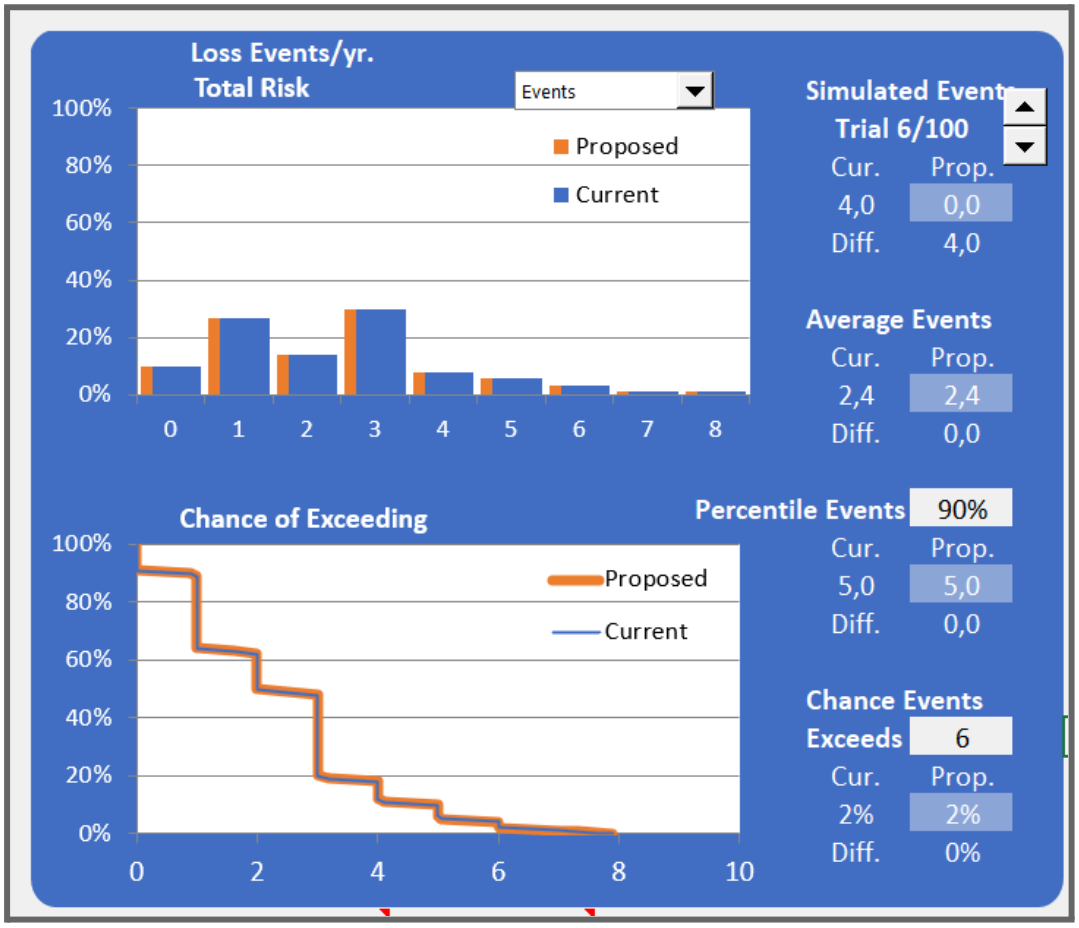
Contact Frequency/yr.	Cur.	Pro.
Min	21	
ML	42	
Max	63	

Probability of Action	Cur.	Pro.
Min	15%	
ML	25%	
Max	35%	

Threat Capability	Cur.	Pro.
Min	16%	
ML	33%	
Max	50%	

Resistance Strength	Cur.	Pro.
Min	25%	
ML	40%	
Max	60%	

Análisis de probabilidades de ocurrencia:



Conclusiones

- ChaseMyCash recibe de media 2 propagaciones de ransomware al año.
- La probabilidad de que suceda al menos 1 evento de este tipo al año es de 93% .
- La probabilidad de que haya más de 4 propagaciones al año es del 19%.
- Es muy poco probable de que en el mismo año ocurra 6 propagaciones de ransomware, con una probabilidad del 3%.

Impacto

Pérdidas primarias

Productividad:

El porcentaje de dinero que no se recibe durante un mes por parte del coste de las licencias de los clientes se ha calculado siguiendo las siguientes estimaciones: Se ha deducido que de los 20.000 clientes el 20% (4.000 clientes) tienen la licencia Premium (100€/año -> 8,33 €/mes), el 30% (6.000 clientes) tienen la licencia Large (75€/año aprox. -> 6,25€/mes). Otro 20% (4.000 clientes) tiene la licencia Medium (50€/año -> 4,16€/mes y el 30% restante (6.000 clientes) tienen la licencia Small (20€/año -> 1,66 €/mes).

Por tanto, ChaseMyCash dejaría de ganar como máximo durante ese mes 97.420€, un promedio de 75.720€/mes (10% Premium, 10% Large, 40% Medium, 40% Small) y un mínimo (20% Large, 30% Medium y 50% Small) de 66.290€/mes.

Para evitar lo máximo posible esta pérdida de productividad se ha pedido a los empleados que hagan horas extras hasta un máximo de 4 horas al día. Siendo estas horas extras pagadas a 35€/hora. Según los datos recogidos en el informe oficial sobre ransomware de Sophos se tarda de media un mes en recuperarse de un ransomware, por lo que el precio promedio en caso de que los 9 empleados de IT hagan las 50 horas extra/mes aproximadamente sería de 15.750€/mes. En el caso máximo de 80 horas extra/mes sería de 25.200€ y el mínimo 20 horas extra/mes de 6.300€.

Reemplazo:

Por norma general el ransomware no ocasiona la necesidad de reemplazo de personal o equipos. Por los que estableceremos un valor mínimo de 2.000€, un valor medio de 5.000€ y un máximo de 7.500€.

Respuesta:

El costo promedio de responder al ransomware puede variar considerablemente dependiendo de la gravedad del ataque y la extensión del daño causado. Por lo general, este costo incluirá el pago del rescate (si se opta por hacerlo), la eliminación del ransomware, la restauración de los datos afectados y la implementación de medidas de seguridad adicionales para prevenir futuros ataques. Se estipula que el costo máximo será de 30.000€, con un promedio de 20.000€ y un mínimo de 10.000€.

Pérdidas secundarias

Probabilidad de pérdidas secundarias:

Dado el mayor riesgo asociado con el uso de dispositivos personales por parte de los empleados, se ajustan los porcentajes para reflejar esta mayor probabilidad. Se establece que la probabilidad mínima de ocurrencia de pérdidas secundarias sea del 20%, con un promedio del 40% y un máximo del 60%.

Respuesta:

Con el objetivo de mitigar las pérdidas secundarias y reducir la probabilidad de futuros ataques de ransomware, se tomará la decisión de adquirir dispositivos móviles empresariales para todos los empleados, los cuales contarán con las medidas de seguridad necesarias. Se ha establecido que el costo mínimo de esta inversión será de aproximadamente 4000€, con un promedio de 6000€ y un máximo de 8000€.

Reputación:

Relacionado con la probabilidad de pérdida secundaria, los costos de reputación se enfocarán en la adquisición de nuevos clientes, lo cual podría resultar desafiante debido a la creación de desconfianza entre los usuarios. Por lo tanto, se requerirá la asignación de recursos adicionales para la captación de nuevos clientes, como campañas de marketing u ofertas en las diversas licencias del producto, con un costo promedio estimado de 3.000€. Se prevé que los clientes más antiguos o aquellos asociados directamente con la empresa seguirán siendo leales. Sin embargo, se estima una pérdida promedio de 20.000€ debido a la

pérdida del 5% de los clientes con las licencias más económicas.

Ventaja competitiva:

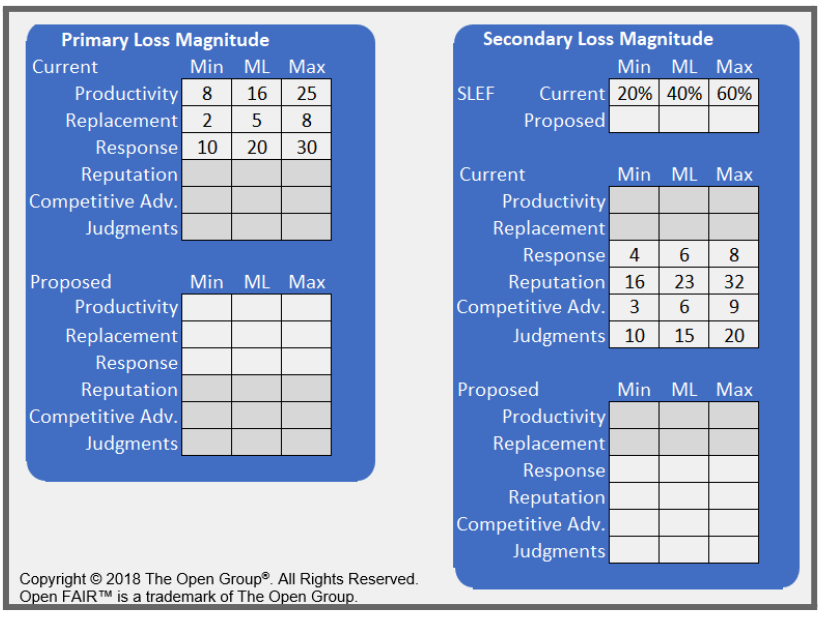
Un ataque de ransomware puede tener un impacto significativo en la capacidad operativa de una empresa, lo que a su vez podría afectar su posición competitiva. Por ejemplo, si una empresa se ve imposibilitada de acceder a sus datos y sistemas durante un período prolongado, podría perder la capacidad de cumplir con los pedidos de los clientes o de responder de manera ágil a las demandas del mercado, lo que potencialmente permitiría a los competidores ganar una ventaja competitiva.

Por tanto, se han establecido valores para cuantificar este impacto. El costo máximo de este impacto se estima en 9.000€, con un promedio de 6.000€ y un mínimo de 3.000€.

Juicios:

Es crucial considerar que el enjuiciamiento de los autores de ransomware puede ser un proceso complejo, costoso y prolongado, que podría requerir la participación de varios departamentos gubernamentales y agencias de aplicación de la ley. El costo promedio asociado a este proceso se estima en 15.000€.

Resumen de los valores utilizados:



Primary Loss Magnitude

Current	Min	ML	Max
Productivity	8	16	25
Replacement	2	5	8
Response	10	20	30
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

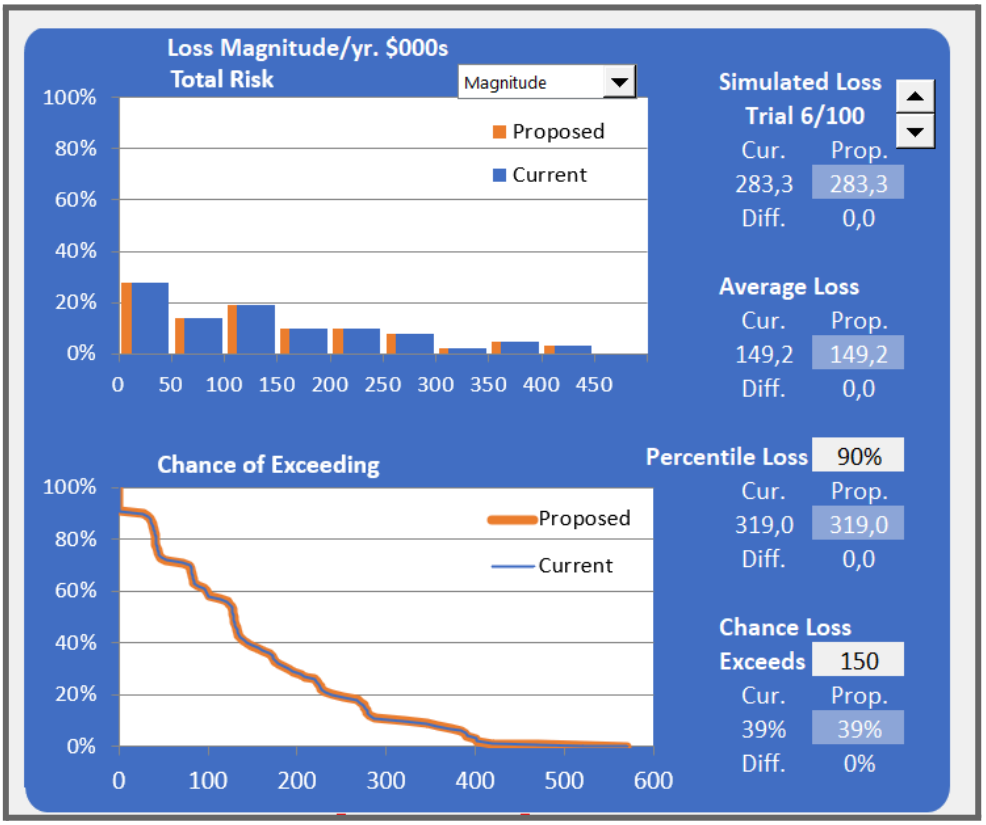
Secondary Loss Magnitude

		Min	ML	Max
SLEF	Current	20%	40%	60%
	Proposed			

Current	Min	ML	Max
Productivity			
Replacement			
Response	4	6	8
Reputation	16	23	32
Competitive Adv.	3	6	9
Judgments	10	15	20

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Análisis del coste estimado:



Conclusiones

- El coste medio que va a suponer para la empresa va a ser de 149.200€ al año
- La probabilidad de que este incidente genere pérdidas, de más de 150.000, es de 39%
- Relativo a los datos el coste máximo que puede asumir la empresa al año es aproximadamente 587.000€.

1.2. BRECHA DE DATOS QUE AFECTA AL CÓDIGO DE LA APLICACIÓN.

Objetivo

El objetivo es estimar la probabilidad e impacto asociados que tendrá nuestra empresa ChaseMyCash en caso de sufrir una brecha de datos debido a un posible acceso no autorizado.

Contexto

Durante un análisis de seguridad llevado a cabo por la empresa, se descubrió que los empleados tenían privilegios de administrador. Esto implicaba que un empleado tenía la capacidad de descargar un archivo infectado con malware en su computadora portátil de trabajo. Este escenario plantea la posibilidad de que un atacante remoto pudiera acceder a la red corporativa y comprometer el código fuente de la aplicación.

Activos

Los activos en riesgo frente a la eventualidad de este incidente incluyen principalmente el código de la aplicación alojado en GitHub, el cual engloba toda la lógica de la aplicación. Otro activo afectado sería la reputación de la compañía, así como la información sensible, dado que el código de la aplicación podría contener datos confidenciales.

Adversario

El potencial adversario podría ser un ciberdelincuente o un grupo cibercriminal con el objetivo de obtener información valiosa del código de la aplicación para su beneficio personal o para perjudicar la reputación de la compañía.

Tipo de amenaza

La naturaleza de la amenaza es maliciosa, ya que los adversarios no deberían tener acceso al código bajo ningún concepto. Por lo tanto, la única manera de obtener acceso sería a través de una intrusión no autorizada en un dispositivo.

Impacto de la amenaza

Principalmente, este riesgo impacta en la confidencialidad, dado que la información del código de la aplicación puede ser expuesta y comprometida. Asimismo, puede afectar a la integridad, ya que el código de la aplicación podría ser modificado por un atacante, lo que conlleva a un comportamiento no deseado de la aplicación. Por último, podría influir en la disponibilidad, dado que una brecha de datos podría resultar en la interrupción del servicio o en la pérdida de datos.

Alcance

Activo en riesgo	Adversario	Tipo de amenazas	Impacto de la amenaza
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Integridad
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Disponibilidad

Análisis

- **Frecuencia de contacto al año**

  Dado que los empleados utilizan portátiles y aplicaciones/servicios de terceros para llevar a cabo sus tareas, la frecuencia de contacto al año es alta, lo que aumenta las oportunidades de una brecha de datos que pueda afectar al código de la aplicación.

  Para salvaguardar la seguridad de la propiedad intelectual de ChaseMyCash, se ha definido una métrica llamada Frecuencia de Acceso, que se refiere al número de veces que terceros acceden de manera no autorizada al código de la aplicación. Tras un extenso análisis y discusión, se determinó que el número promedio de accesos no autorizados al código sería de 2 por año, considerando diversas posibilidades de vulnerabilidad como el robo de portátiles empresariales y la presencia de malware en los equipos.

  Además, se ha establecido un límite máximo de 5 accesos no autorizados al código por año, con el objetivo de reducir el riesgo de exposición y pérdida de la propiedad intelectual de ChaseMyCash. Se ha acordado también que la frecuencia mínima de incidentes sería de al menos una vez cada tres años, lo que permitirá a ChaseMyCash identificar y abordar cualquier debilidad en sus sistemas de seguridad, garantizando así la protección continua de su propiedad intelectual.

- **Probabilidad de Acción**

  Existen diversas formas en las que un adversario podría intentar obtener acceso al

código de la aplicación, incluyendo el phishing, el malware, la explotación de vulnerabilidades o el robo del dispositivo.

Dado que no todos los empleados de la empresa son programadores y, por lo tanto, no todos necesitan acceso al código, se ha limitado considerablemente la probabilidad de acción. Con 9 programadores dentro de una organización de un total de 18 empleados, el máximo de acceso al código se estableció en un 50%, ya que la mitad de los empleados tendrían dicho acceso. Considerando esta limitación y el hecho de que estos empleados pueden estar sujetos a medidas de seguridad adicionales, como la autenticación multifactorial, se podría establecer un porcentaje medio del 25%. Además, se establece un porcentaje mínimo del 10%, reconociendo que siempre existe la posibilidad de que un adversario logre acceder al código de la aplicación, independientemente de las medidas de seguridad implementadas.

- **Capacidad de Amenaza**

La capacidad de amenaza puede variar significativamente, ya que depende de la habilidad y los recursos del adversario. Sin embargo, se considera que puede ser alta debido a la presencia de numerosos actores malintencionados interesados en obtener información valiosa del código de la aplicación.Si tomamos en cuenta que el atacante posee conocimientos avanzados en ciberseguridad, la capacidad de amenaza aumentaría considerablemente, ya que es probable que requiera menos tiempo para acceder a dicha información sensible o valiosa.

Por lo tanto, se establece un rango de probabilidad de entre el 30% y el 90% para reflejar esta variabilidad en la capacidad de amenaza.

- **Fuerza de Resistencia**

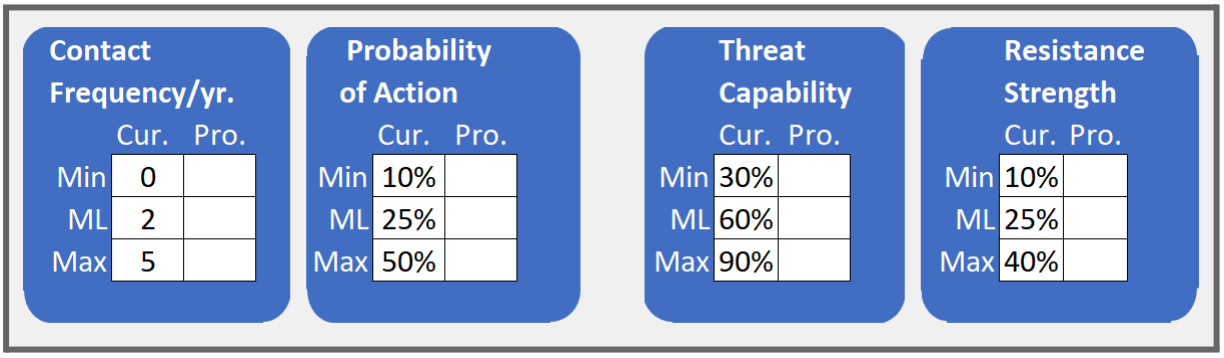
En el proceso de establecer los valores de seguridad para este aspecto, se ha dado prioridad a evitar la extracción y eliminación del código en caso de acceso no autorizado al dispositivo. Se ha identificado que solo dos medidas son cruciales para lograr este propósito: la contraseña de inicio de sesión del dispositivo y las credenciales de GitHub.

No obstante, se ha observado que la política de seguridad de contraseñas de ChaseMyCash es relativamente laxa, ya que solo requiere la inclusión de un número, una letra minúscula y una mayúscula, sin especificar una longitud mínima. Esta situación podría propiciar la elección de contraseñas débiles por parte de empleados descuidados. Además, existe el riesgo de que las credenciales de

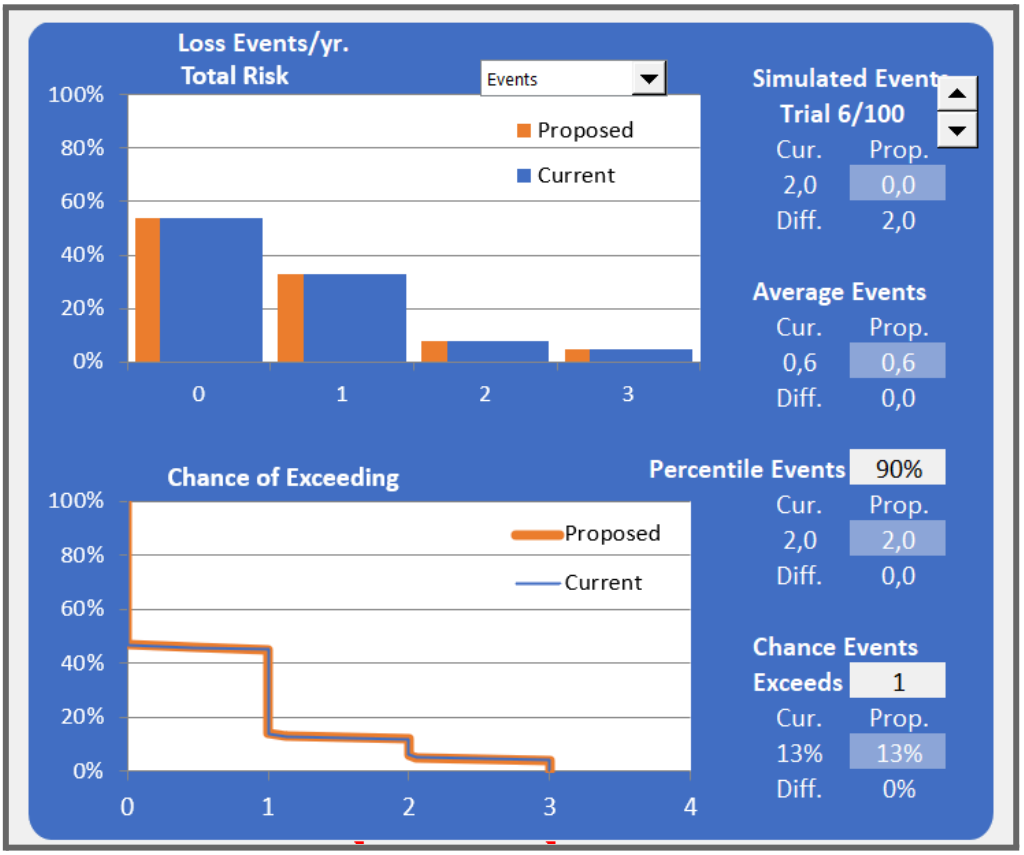
GitHub estén almacenadas en el dispositivo, lo que podría facilitar el acceso no autorizado.

Con el fin de garantizar una protección adecuada, se ha establecido un rango de valores de resistencia que oscila entre el 10% y el 40%, considerando que el 25% es el valor más probable. De esta manera, se busca asegurar que, incluso en caso de robo del dispositivo o compromiso de las medidas de seguridad, el código pueda estar protegido en una proporción significativa.

Resumen de los valores utilizados:



Análisis de probabilidades de ocurrencia:



Conclusiones:

- La empresa tendrá una brecha que afecte al código de 1 vez cada año y medio de promedio
- La probabilidad de que al menos suceda un evento de este tipo al año es de 46%. En cambio la probabilidad de que pase más de 1 vez es del 13%
- La probabilidad de que suceda el mismo año 2 veces la misma brecha es de 5%
- Muy poco probable que ocurra es veces este incidente al año ya que la probabilidad de ocurrencia es <1%

Impacto

Pérdidas primarias

- **Productividad**

  Se espera que se produzcan pérdidas significativas en productividad, dado que, según la política de la empresa, las copias de seguridad se realizan manualmente y con cierta periodicidad. Esto implica que, en caso de cualquier error catastrófico, se perdería una cantidad considerable de información crítica, ya que no habría una versión reciente disponible para su restauración. Como resultado, se requeriría un extenso esfuerzo para reconstruir el código perdido, lo que podría implicar un período prolongado de tiempo dedicado a este fin.

  Se ha estimado que, para compensar esta pérdida de productividad, los 9 desarrolladores necesitarían trabajar a tiempo completo durante 2 meses. Con un salario estimado de 6000€ por desarrollador, las pérdidas durante estos dos meses se calcularían en aproximadamente 54.000€.

- **Remplazo**

  Ante una situación de tal magnitud y con el objetivo de acelerar la producción, se tomará la decisión de contratar personal adicional, lo que generará nuevos gastos relacionados con el pago de salarios de estas personas, así como la adquisición de nuevos portátiles. Estos gastos adicionales representarán una carga financiera para una empresa de tamaño pequeño, la cual tardará en recuperarse de los mismos. Se estima que, en promedio, estos costos ascenderán a alrededor de 60.000€. Este cálculo incluye la contratación de 2 nuevos empleados junto con el costo asociado de adquirir los portátiles necesarios para su trabajo.

- **Respuesta**

  Con el objetivo de prevenir problemas similares en el futuro, se llevarán a cabo pruebas de intrusión, lo que implicará gastos adicionales de respuesta dependiendo del alcance de dichas pruebas y la complejidad del incidente. Determinar la naturaleza del ataque y los datos comprometidos podría requerir la intervención de expertos en seguridad informática. Los costos asociados a estas pruebas pueden variar entre los 15.000€ y los 40.000€ (valor máximo), con un costo promedio estimado de 27.500€.

Pérdidas secundarias

- **Probabilidad de pérdida secundaria:**

  Como pérdida secundaria, se considera el impacto en la imagen y la reputación de la empresa, que sufriría un daño significativo como resultado de estos eventos. Se estima que en el 50% de las ocasiones será necesario emplear recursos adicionales para mitigar los efectos adversos en la imagen y la reputación de la empresa.

- **Respuesta:**

  La contratación de un proyecto forense con el fin de determinar las causas del incidente y prevenir su recurrencia implica gastos adicionales de respuesta. Se estima que el gasto promedio para este tipo de contratación será de unos 15.000€.

- **Reputación:**

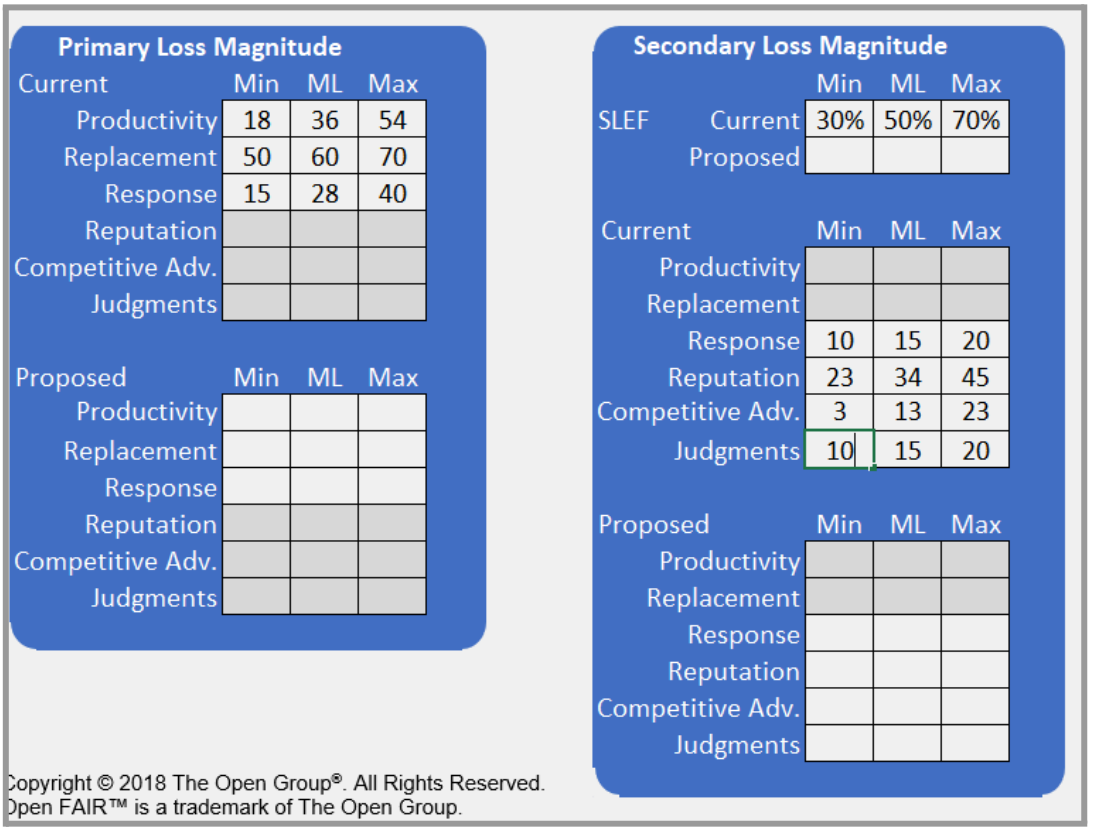
  Los gastos relacionados con la reputación se centran en la captación de nuevos clientes. Esta tarea sería difícil debido a que se generarían sentimientos de desconfianza entre los usuarios existentes. Por lo tanto, será necesario destinar recursos adicionales para atraer nuevos clientes, como campañas de marketing u ofertas en las diferentes licencias del producto, con un costo promedio estimado de 3.500€.

  Se prevé que los clientes más antiguos o las entidades relacionadas con la empresa seguirán siendo leales. Sin embargo, se estima una pérdida promedio de 30.000€ debido a la pérdida del 5% de los clientes que utilizan las licencias más económicas.

- **Ventaja competitiva:**
  La capacidad de querer destacar frente a otras empresas será complicado de implementar ya que se verá estancado durante los 2 meses que se están invirtiendo para reconstruir el código de la app. En este tiempo se prevé que 250 clientes nuevos con un precio medio de 50€ por suscripción lo que sería 12.500€.

- **Juicios:**
  Los procedimientos legales estarán condicionados por los resultados obtenidos de la prueba forense. Si se demuestra que el incidente fue provocado por una empresa externa, se iniciará un proceso judicial. Se ha establecido un valor promedio para este tipo de acciones legales en 15.000€.

Resumen de los valores utilizados:



Primary Loss Magnitude

Current	Min	ML	Max
Productivity	18	36	54
Replacement	50	60	70
Response	15	28	40
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

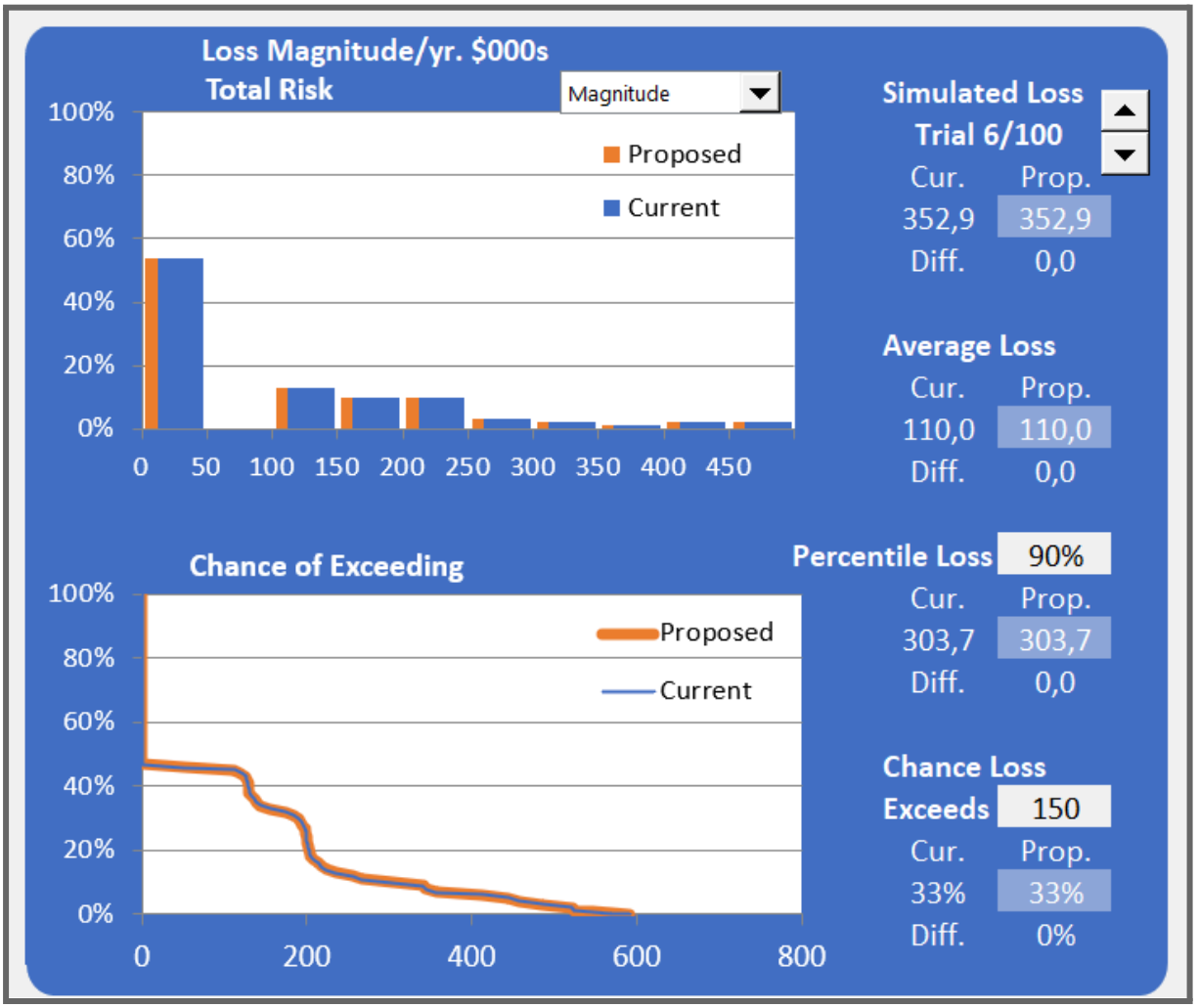
Secondary Loss Magnitude

SLEF	Min	ML	Max
Current	30%	50%	70%
Proposed			

Current	Min	ML	Max
Productivity			
Replacement			
Response	10	15	20
Reputation	23	34	45
Competitive Adv.	3	13	23
Judgments	10	15	20

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Análisis del coste estimado:



Conclusiones:

- El coste medio que supone para la empresa es de 110.000€
- La probabilidad de que el incidente genere más de 150.000€ de pérdida es del 33%.
- El coste máximo que se puede asumir anualmente a causa de esta brecha por ChaseMyCash sería de 599.000€. El doble de lo que la empresa genera anualmente.

2. SEGURIDAD DEL PRODUCTO

2.1 BRECHA DE DATOS CLIENTES

Objetivo

El propósito es detectar los riesgos y consecuencias potenciales vinculados a una eventual filtración de información confidencial del cliente, originada por un acceso no autorizado tanto a la base de datos como al servicio de almacenamiento

Contexto

Durante una revisión interna de pruebas de penetración, los informes revelaron un hallazgo preocupante: se encontraron ciertos puertos accesibles desde el exterior, incluido el puerto 3306. Además, se observó que el servicio de almacenamiento utilizado (bucket de Amazon S3) estaba configurado de manera que no cifraba ningún elemento almacenado en él. Este informe se calificó como extremadamente grave.

Activos en riesgo

Los datos en riesgo incluyen toda la información necesaria para iniciar sesión de los usuarios (nombres de usuario, correos electrónicos, contraseñas, roles, permisos, etc.), así como información personal relacionada con sus objetivos, preferencias y alertas configuradas. Además, los archivos XLS o CSV cargados por los usuarios, así como archivos que contienen facturas, declaraciones de impuestos y otros documentos similares almacenados en el bucket, también están en peligro. Esta situación afectará no solo a la información sensible, sino también a la reputación tanto del cliente como de la compañía.

Adversario

El adversario puede ser cualquier individuo o grupo que busque obtener acceso no autorizado a la información almacenada en la base de datos de la empresa. Esto podría incluir hackers, empleados deshonestos o cualquier persona con acceso a la red o los dispositivos de la empresa. Además, no se puede descartar la posibilidad de que un empleado con acceso legítimo tenga intenciones maliciosas.

Tipo de amenaza

La amenaza puede darse de forma accidental, como cuando un empleado no sigue los procedimientos de seguridad establecidos o debido a debilidades en el software utilizado. Lo que podría resultar en una filtración de datos. Sin embargo, en la mayoría de los casos, el peligro proviene de un ataque deliberado por parte de un hacker informático que busca acceder a información confidencial y comprometer la seguridad de la empresa.

Impacto de la amenaza

Una violación de datos de clientes tiene un impacto primordial en la confidencialidad, ya que la información personal de los clientes corre el riesgo de ser comprometida, lo que potencialmente puede amenazar su privacidad y seguridad. En términos de integridad, los datos almacenados en la base de datos pueden ser alterados o eliminados, lo que podría resultar en pérdidas de información crítica. Por último, en lo que respecta a la disponibilidad, una brecha de datos de clientes podría resultar en una negación de servicio, ya que los sistemas de la empresa podrían verse afectados y no estar disponibles para su funcionamiento normal.

Alcance

ACTIVO EN RIESGO	ADVERSARIO	TIPO DE AMENAZAS	IMPACTO DE LA AMENAZA
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Integridad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad

ANÁLISIS.

- ### Frecuencia de contacto al año.

  Según la definición en la tabla anterior, los agentes involucrados en estas actividades son externos. Por esta razón, la frecuencia de contacto se ha definido como el número de consultas o intentos de acceso a la base de datos desde direcciones IP no registradas en la lista blanca, es decir, desde dispositivos o redes externas que no han sido previamente autorizadas y que podrían ser potencialmente maliciosas. Dado que el puerto 3306 está expuesto a Internet y que ningún elemento almacenado en el bucket de S3 está cifrado, es posible que los atacantes intenten acceder a la base de datos en busca de información valiosa de los clientes. Por lo tanto, se estima que la frecuencia media de intentos de acceso no autorizado podría ser de 50 intentos por día, lo que equivaldría a un promedio de 18.250 intentos de acceso no autorizado por año.

- ### Probabilidad de acción.

  Hemos identificado diversas amenazas relacionadas con este riesgo. Desde un atacante que obtiene acceso a datos no autorizados hasta posibles empleados que puedan filtrar algún tipo de información. Dado que hay varias formas de lograr el mismo objetivo y considerando ciertas debilidades en la empresa, hemos establecido un valor promedio moderado del 40% para estas amenazas.

- ### Capacidad de amenaza.

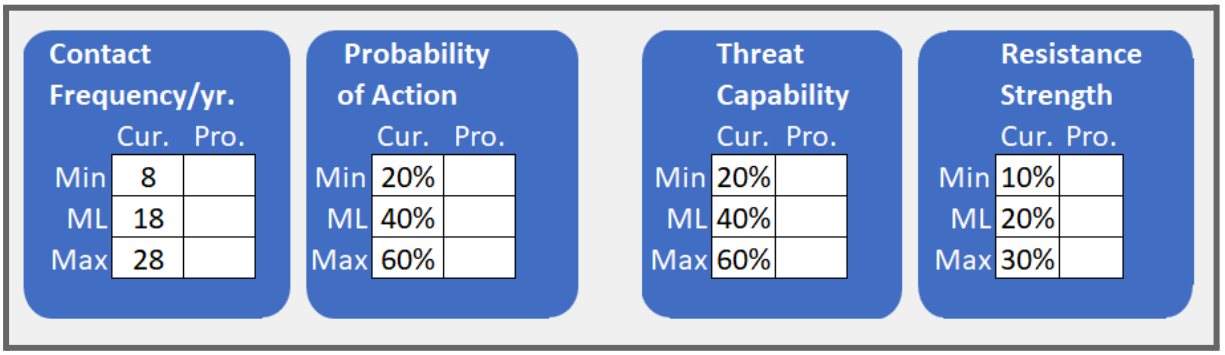
  Por un lado, si el atacante posee un alto nivel de habilidades técnicas, podría aprovechar una configuración de seguridad inadecuada para explotar vulnerabilidades y obtener así información valiosa de la base de datos de clientes. Por lo tanto, la capacidad de amenaza dependerá de la motivación y habilidades del atacante. Considerando todos estos aspectos, estimamos que la capacidad de amenaza tendrá un porcentaje medio del 40%.

- ### Fuerza de resistencia.

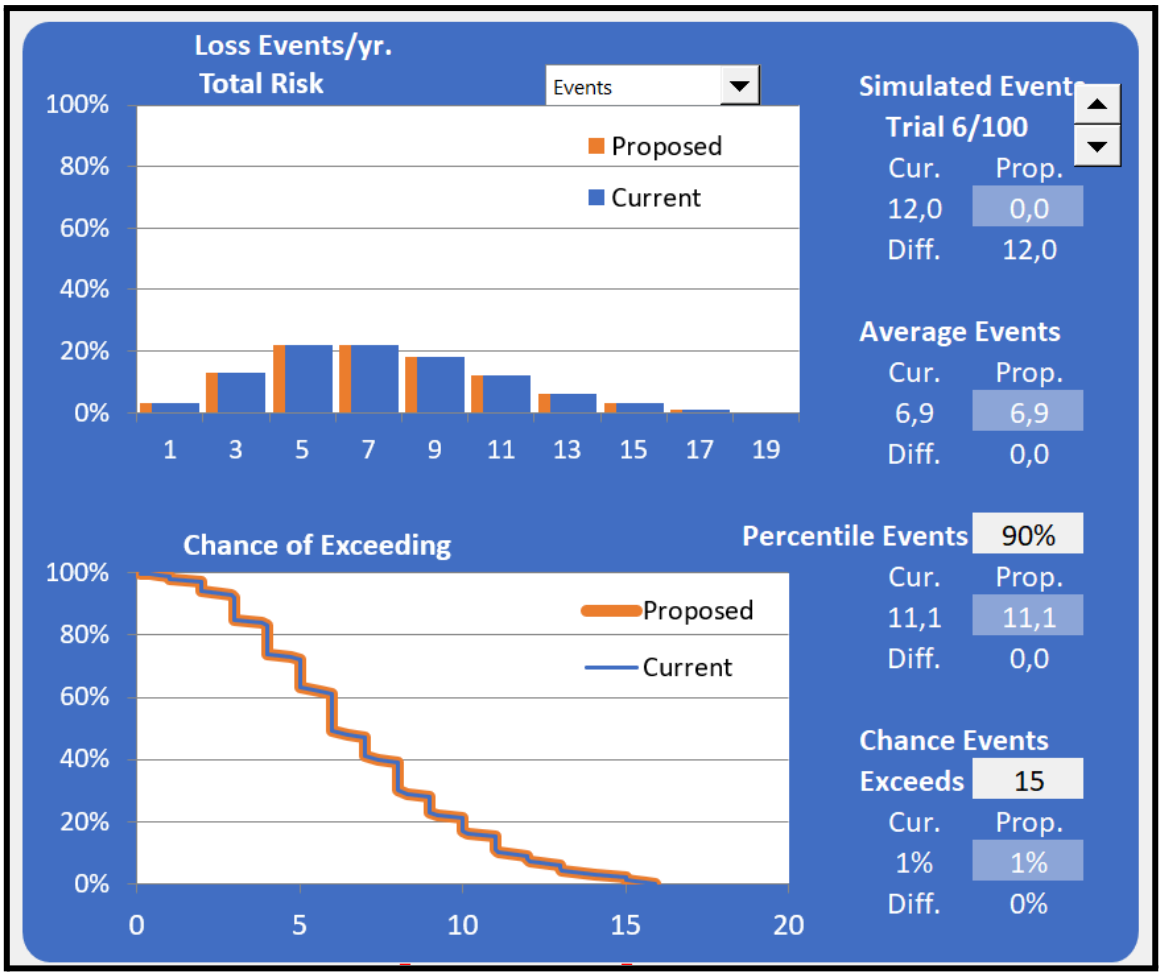
  Además de las debilidades identificadas en relación con el puerto 3306 y el cifrado del bucket, se suma la ausencia de una política de eliminación de elementos, lo cual también representa un riesgo. Sin embargo, existen controles como el cifrado en reposo en AWS RDS o el uso de JSON Web Token para autenticación, así como la gestión de permisos personalizados en ExpressJS, que pueden contribuir a reducir la probabilidad de una brecha de seguridad. A pesar

de estas medidas existentes, se considera que aún son insuficientes, por lo tanto, estimamos una fuerza de resistencia media del 20%

RESUMEN VALORES UTILIZADOS



ANÁLISIS PROBABILIDADES DE OCURRENCIA



CONCLUSIONES

- Observamos que la información de los clientes de la empresa podría ser expuesta una media de 6 veces al año
- La probabilidad de que al menos suceda un evento de este tipo es del 97% al año
- La probabilidad de que esta clase de eventos ocurra 15 veces al año es extremadamente baja (1%).
- La probabilidad de que haya más de 8 brechas de datos de clientes al año es del 29%.

IMPACTO

PÉRDIDAS PRIMARIAS

- **Productividad**

  Cuando ocurren este tipo de incidentes, los programadores y otros miembros del equipo de tecnología de la empresa pueden encontrarse en la necesidad de dedicar una cantidad considerable de tiempo y esfuerzo para abordar el problema.

  Este impacto en la productividad puede generar costos financieros significativos para la empresa, ya que las operaciones normales pueden experimentar retrasos, lo que posiblemente requiera el pago de horas extras a los trabajadores para cumplir con los plazos de entrega. Por lo tanto, se estima que el costo promedio de la pérdida de productividad sería de 15.000€

- **Reemplazo**

  En cuanto al reemplazo del personal, consideraremos valores bajos, ya que generalmente no es necesario sustituir al personal ante una situación de este tipo. Esto se debe a que no se considera que la falta de seguridad al 100% sea completamente culpa de los desarrolladores. Sin embargo, en el caso excepcional de que sea necesario, tendríamos que cubrir el salario de un nuevo empleado y el finiquito de la persona despedida. Por lo tanto, estimaremos un costo promedio de 10.000€, con un mínimo de 5.000€ y un máximo de 15.000€

- **Respuesta**

  Es crucial que la empresa tome medidas adecuadas para fortalecer la seguridad de sus sistemas y datos. Para mitigar el riesgo de una brecha de datos, la empresa podría implementar medidas adicionales de seguridad, como el cifrado

de datos almacenados en el bucket S3 y la restricción del acceso a puertos no esenciales, como el puerto 3306.Por otro lado, la empresa podría enfrentar multas y sanciones por no proteger adecuadamente los datos de sus clientes o por incumplir con las regulaciones de privacidad. Además, podría ser necesario que la empresa pague indemnizaciones a las personas afectadas por el robo de datos. Ante todas estas posibles eventualidades, estableceremos un costo mínimo de 20.000€, un costo promedio de 45.000€ y un costo máximo de 65.000€.

PÉRDIDAS SECUNDARIAS

- **Probabilidad de pérdida secundaria**

  Entre ellos, destacan los costos de notificación y cumplimiento. La empresa podría incurrir en gastos significativos relacionados con la notificación a los clientes, la realización de investigaciones, la implementación de medidas de seguridad adicionales y el cumplimiento de las regulaciones. Por otro lado, los clientes afectados por la filtración de datos podrían presentar demandas contra la empresa por daños y perjuicios, lo que podría resultar en costos legales significativos y dañar aún más la reputación de la empresa. Por lo tanto, se ha estimado un valor promedio del 30% para estos costos secundarios.

- **Respuesta**

  Para evitar futuros ataques de este tipo, es importante que la empresa implemente medidas adicionales. Por ejemplo, se sugiere establecer políticas claras de eliminación de datos y configurar copias de seguridad automáticas para asegurar que los datos críticos estén respaldados y eliminados de manera oportuna. Se estima un costo promedio de 4.000€ para implementar estas medidas, con un rango mínimo de 2.000€ y máximo de 6.000€.

- **Reputación**

  Tomando en cuenta una posible pérdida de reputación significativa, si la empresa emite un comunicado explicando el problema ocurrido, es probable que muchos clientes perciban a la empresa como vulnerable y poco confiable en términos de seguridad, lo que podría resultar en la pérdida de clientes. Ante esta situación, será necesario invertir recursos adicionales en la atracción de nuevos clientes, lo que podría incluir el desarrollo de estrategias de marketing específicas para recuperar la confianza del mercado y atraer a nuevos clientes.

Estimamos un costo promedio de 4.000€ para implementar estas estrategias de recuperación de reputación y atracción de nuevos clientes.

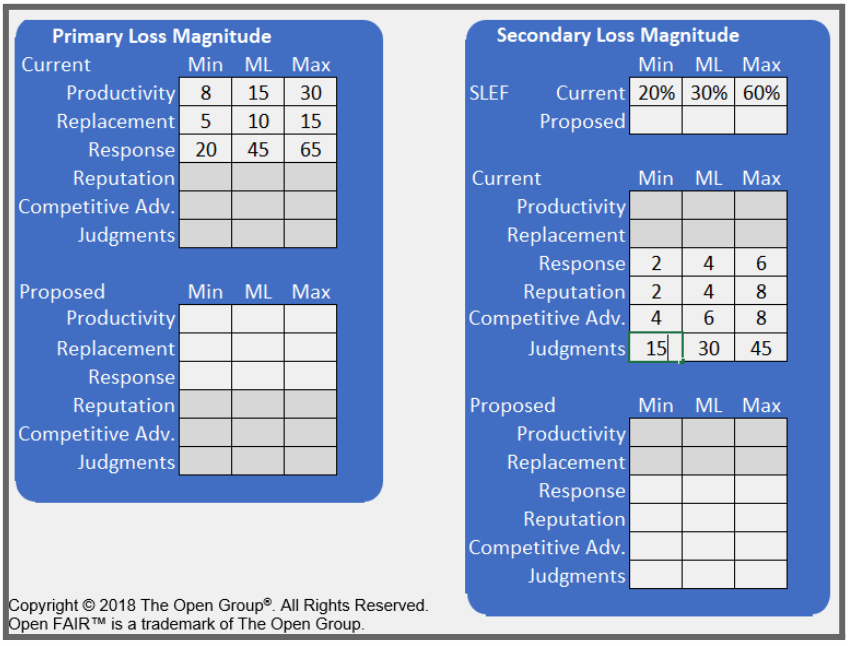
- **Ventaja competitiva**

  Dado que se trata de información de clientes, es poco probable que la ventaja competitiva de la empresa se vea especialmente afectada, ya que estos datos no proporcionan ninguna información relevante para las empresas competidoras. Sin embargo, como consecuencia negativa, estas empresas competidoras podrían aprovechar la filtración de datos para desarrollar campañas publicitarias dirigidas específicamente a los clientes afectados.

- **Juicios**

  Dado que la información expuesta corresponde a datos de clientes, la empresa enfrentará gastos legales significativos. ChaseMyCash podría enfrentar multas por no cumplir con las regulaciones de privacidad, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Estas multas podrían ser significativas y dependerán del número de usuarios afectados, la gravedad de la violación y la naturaleza de los datos expuestos. Además, la empresa podría enfrentar demandas por parte de los clientes cuyos datos se vieron comprometidos en la brecha. Los costos legales asociados pueden establecer un costo promedio estimado de alrededor de 30.000€ para cubrir estos gastos legales.

RESUMEN DE LOS VALORES UTILIZADOS



Primary Loss Magnitude

Current	Min	ML	Max
Productivity	8	15	30
Replacement	5	10	15
Response	20	45	65
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

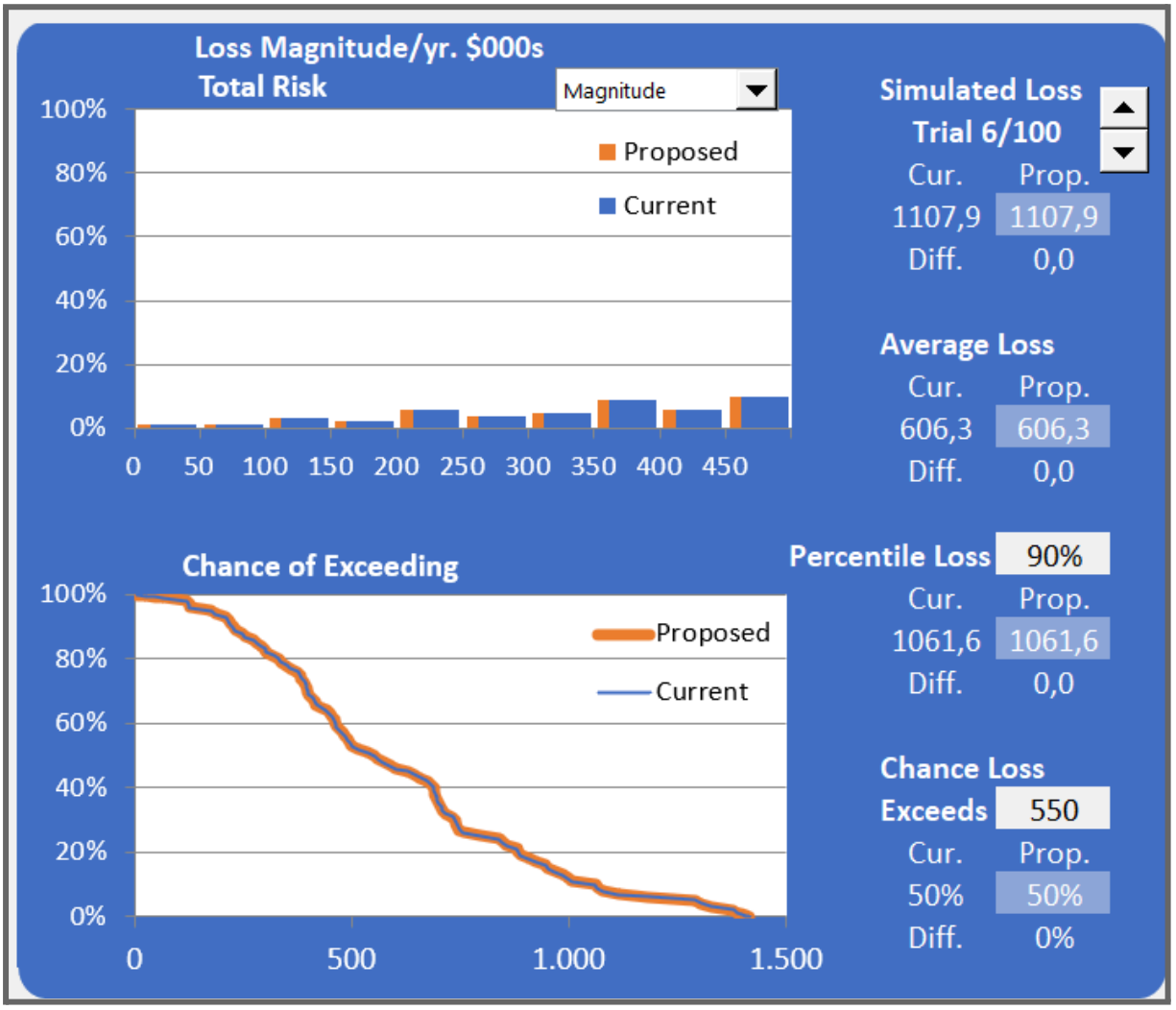
Secondary Loss Magnitude

		Min	ML	Max
SLEF	Current	20%	30%	60%
	Proposed			

Current	Min	ML	Max
Productivity			
Replacement			
Response	2	4	6
Reputation	2	4	8
Competitive Adv.	4	6	8
Judgments	15	30	45

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

ANÁLISIS COSTE ESTIMADO



CONCLUSIONES

- El coste medio que supondría para la empresa sería de 606.300€ al año.
- La probabilidad de que en un año este incidente genere pérdidas de más de 700.000€ sería del 35%.
- El coste máximo que la empresa puede asumir al año es aproximadamente de 1.415.000€ que supone casi 5 veces la facturación anual.

2.2 DENEGACIÓN DE SERVICIOS

Objetivo

El objetivo es evaluar el riesgo de denegación de servicio provocado por la eliminación accidental de datos de la base de datos. Esto podría conducir a la pérdida de acceso a información sensible de los usuarios, como datos de inicio de sesión, información personal y detalles del producto. Es crucial analizar este riesgo para prevenir interrupciones en el servicio y salvaguardar la reputación tanto de la empresa como de sus clientes.

Contexto

La empresa ha identificado que la ausencia de una política de eliminación automática de elementos en la base de datos, junto con la realización manual de copias de seguridad, podría incrementar el riesgo de una eventual denegación de servicio en caso de un fallo en la base de datos.

Activos en riesgo

El activo en riesgo es la reputación de la empresa. Una denegación de servicio podría comprometer la disponibilidad del servicio y ocasionar insatisfacción entre los clientes, lo que eventualmente podría perjudicar la imagen y reputación de la compañía

Tipo de amenaza

En este caso, la amenaza podría ser tanto accidental como intencionada. Una eliminación accidental de la información de la base de datos podría ser causada por un error humano o técnico, mientras que una eliminación intencional podría ser causada por un usuario malintencionado o un atacante externo.

Impacto de la amenaza

En términos de integridad, una interrupción del servicio podría ocasionar la pérdida o corrupción de datos, lo cual afectaría la confiabilidad de la empresa. En relación a la disponibilidad, una denegación de servicio impactaría directamente la capacidad de la empresa para ofrecer sus servicios, lo que podría resultar en consecuencias financieras negativas.

Alcance

ACTIVO EN RIESGO	ADVERSARIO	TIPO DE AMENAZAS	IMPACTO DE LA AMENAZA
Servicios de ChaseMyCash	Persona/Grupo externo/interno	Intención maliciosa/accidental	Disponibilidad
Datos de ChaseMyCash	Persona/Grupo externo/interno	Intención maliciosa/accidental	Integridad

ANÁLISIS

- ### Frecuencia de contacto al año

  La frecuencia de contacto se interpreta como la cantidad de días al año en los que un usuario legítimo no puede acceder al servicio ofrecido por la empresa debido a una denegación de servicio, sin importar la causa. Esta métrica nos ayuda a evaluar la disponibilidad de la aplicación de la empresa.

  En este contexto, la frecuencia de contacto se utiliza para valorar la calidad y fiabilidad de un servicio digital. Se ha establecido que, en promedio, la empresa no puede ofrecer sus servicios durante 12 días al año, con un mínimo de 6 días y un máximo de 24 días.

- ### Probabilidad de acción.

  La posibilidad de que un adversario lleve a cabo un ataque de denegación de servicio varía según varios factores, como la visibilidad de la empresa, la naturaleza de su actividad y si hay alguien motivado para realizar dicho ataque. Otros elementos que pueden contribuir a estos ataques incluyen fallas en la infraestructura, errores de programación y la falta de medidas de seguridad adecuadas, como la ausencia de políticas de copias de seguridad. Por consiguiente, la probabilidad media de que se produzca una acción de este tipo se estima en alrededor del 35%, con un mínimo del 20% y un máximo del 45%.

- ### Capacidad de amenaza.

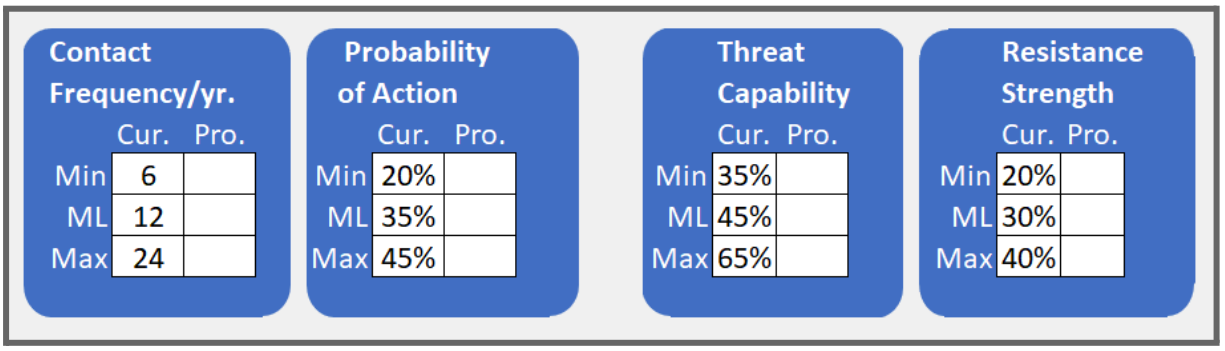
  En general, la capacidad de amenaza en un ataque DDoS es alta, ya que los atacantes pueden aprovechar herramientas automatizadas para inundar el sistema con tráfico malintencionado y sobrecargar la infraestructura de la

empresa, lo que podría resultar en una interrupción del servicio y dejar la aplicación inoperable.Además, los ataques DDoS están siendo cada vez más frecuentes y sofisticados, lo que implica que las empresas deben estar preparadas para enfrentar este tipo de amenazas y tomar medidas preventivas para reducir la probabilidad de interrupciones en el servicio. Por todo lo mencionado, la capacidad de amenaza se sitúa en un nivel moderado, con un valor promedio del 45%.

- **Fuerza de resistencia.**

Se puede deducir que la infraestructura de AWS empleada para hospedar la aplicación, incluyendo AWS VPC, podría ofrecer cierta protección contra ataques de denegación de servicio distribuido (DDoS). AWS proporciona servicios como AWS Shield y AWS WAF que pueden ayudar a salvaguardar las aplicaciones web contra tales ataques. Además, es plausible que la empresa haya implementado algún tipo de mitigación de DDoS en su capa de red o en la capa de aplicación. Sin embargo, es importante destacar que todos los empleados cuentan con permisos de administrador, lo que podría resultar en la eliminación completa de la base de datos y dejar el servicio inoperativo en caso de un error humano. Se estima un porcentaje medio de este riesgo en un 30%.

RESUMEN VALORES UTILIZADOS



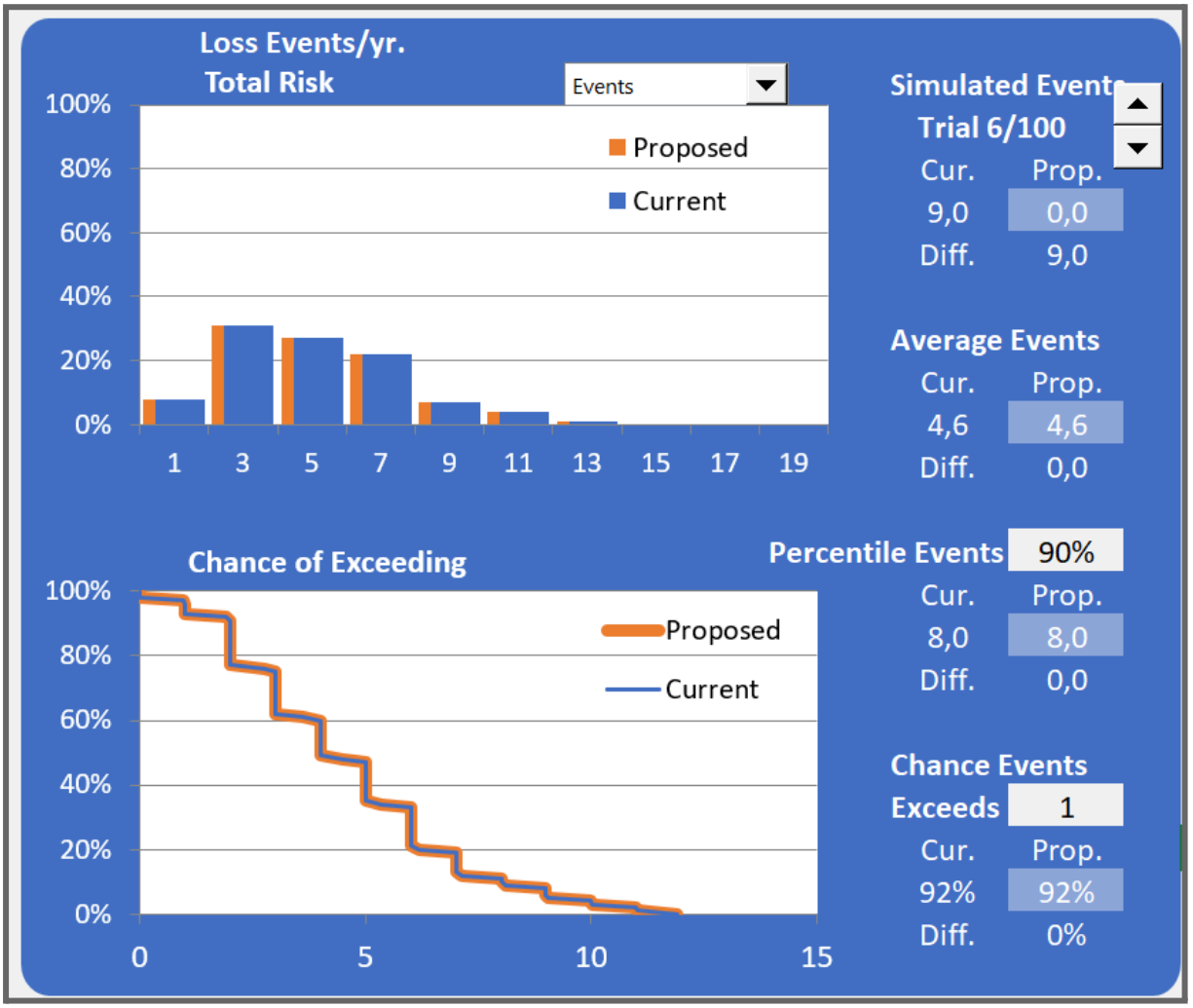
Contact Frequency/yr.	Cur.	Pro.
Min	6	
ML	12	
Max	24	

Probability of Action	Cur.	Pro.
Min	20%	
ML	35%	
Max	45%	

Threat Capability	Cur.	Pro.
Min	35%	
ML	45%	
Max	65%	

Resistance Strength	Cur.	Pro.
Min	20%	
ML	30%	
Max	40%	

ANÁLISIS PROBABILIDADES DE OCURRENCIA



CONCLUSIONES

- La empresa ChaseMyChash de media sufrirá aproximadamente cada año una media de 5 días (120 horas) de tiempo de denegación de servicio.
- La probabilidad de que la empresa sufra un DDoS durante un día al año es del 92%.
- Es muy poco probable (5%) que en el mismo año este incidente provoque 9 días de denegación.
- Es prácticamente imposible que haya más de 11 días de indisponibilidad al año, puesto que su probabilidad es inferior al 1%.

IMPACTO

PÉRDIDAS PRIMARIAS

- ### Productividad

  Una denegación de servicio puede tener un impacto perjudicial en la productividad de una empresa, ya que puede afectar no solo los servicios en línea de la empresa, sino también sus procesos internos, como el correo electrónico, el intercambio de archivos y otras herramientas de colaboración. Esto puede conducir a la interrupción de la comunicación entre los empleados y a la desaceleración de los procesos internos, lo que a su vez puede afectar la productividad en general. Se estima un costo promedio asociado a esta pérdida de productividad de 15.000€

- ### Reemplazo

  Este tipo de ataque no suele ocasionar la necesidad de reemplazo de ningún equipo. En caso de que el borrado haya sido producido de manera intencional por parte de un empleado será necesario su despido, añadiendo a los gastos el finiquito además de la contratación de un nuevo empleado. Por lo tanto el coste medio será de unos 30.000€, el coste mínimo de 20.000€ y el coste máximo de 40.000€.

- ### Respuesta

  Es crucial que la empresa tome medidas adecuadas para mejorar la seguridad de sus sistemas y garantizar la disponibilidad de sus servicios. Con el fin de minimizar el riesgo de una denegación de servicio, la empresa podría implementar medidas de seguridad adicionales, como contratar el servicio de AWS Shield, con un costo medio anual estimado de alrededor de 37.200€. Además, se podría llevar a cabo una revisión de los permisos de todos los empleados para evitar posibles fallos de eliminación parcial o total de la base de datos. Asimismo, se recomendaría establecer un plan de copias de seguridad regulares con alta capacidad de recuperación, lo que supondría un costo adicional de aproximadamente 500€ anuales. En resumen, el costo promedio total estimado para implementar estas medidas sería de 40.000€, con un mínimo de 30.000€ y un máximo de 55.000€. Estas inversiones son fundamentales para proteger los sistemas de la empresa y garantizar la continuidad de sus operaciones frente a posibles amenazas de denegación de servicio.

PÉRDIDAS SECUNDARIAS

- **Probabilidad de pérdida secundaria:**

  Cuando una empresa experimenta una denegación de servicio, las pérdidas secundarias pueden ser significativas. Además de la interrupción temporal de los servicios y la pérdida de productividad, la empresa puede enfrentar costos de recuperación. Esto implica invertir en tecnología y recursos adicionales para recuperarse del ataque, lo que conlleva costos adicionales.

  Además, podría producirse la interrupción de operaciones críticas. Dado que la empresa depende de tecnología y sistemas críticos para sus operaciones diarias, una denegación de servicio podría interrumpir estos sistemas y causar problemas significativos.

  Debido a estos factores, hemos calculado que dichas pérdidas secundarias se producirán, en promedio, el 35% de las veces.

- **Respuesta:**

  En cuanto a las respuestas secundarias después de una denegación de servicio, estas incluyen la actualización de software y sistemas, la implementación de medidas de seguridad adicionales y la capacitación del personal en seguridad informática. Por lo tanto, calculamos que el costo promedio de estas acciones sería de alrededor de 3.000€.

- **Reputación:**

  Consideramos que un deterioro significativo en el prestigio de la compañía podría ocurrir, ya que si la empresa emite una declaración para aclarar el incidente, es probable que muchos consumidores perciban a la organización como débil y poco confiable en términos de seguridad, lo que podría llevarlos a abandonarla.

  Ante este escenario, será necesario asignar recursos adicionales para la captación de nuevos consumidores. Esto podría implicar la creación de estrategias de publicidad específicas destinadas a atraer a nuevos clientes y restaurar la confianza en el mercado. Se estima que el costo promedio de estas acciones sería de 5.000€.

- **Ventaja competitiva:**

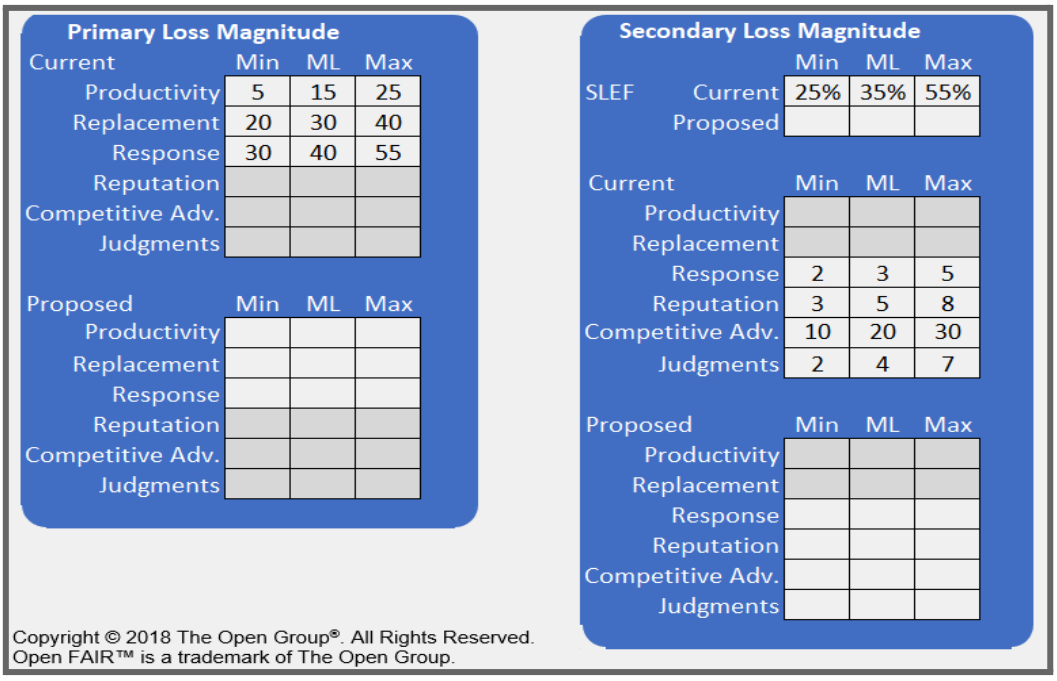
  Una denegación de servicio puede impactar significativamente la capacidad de la empresa para cumplir con sus compromisos adquiridos con los clientes. El tiempo de inactividad resultante puede afectar la

percepción de la empresa por parte de los clientes y disminuir su confianza en la misma. Esto podría resultar en la pérdida de clientes y una reducción en las ventas. Además, si la empresa no logra recuperarse del ataque de manera efectiva, podría perder su ventaja competitiva en el mercado, ya que los clientes podrían optar por competidores que puedan ofrecer servicios similares sin interrupciones. Se estima que el costo promedio de estos impactos sería de 20.000€.

- **Juicios:**

  Si se logra identificar la fuente de la denegación de servicio, es posible emprender acciones legales. Se estima que el costo medio aproximado de tales acciones legales sería de 4.000€.

RESUMEN DE LOS VALORES UTILIZADOS



Primary Loss Magnitude

Current	Min	ML	Max
Productivity	5	15	25
Replacement	20	30	40
Response	30	40	55
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

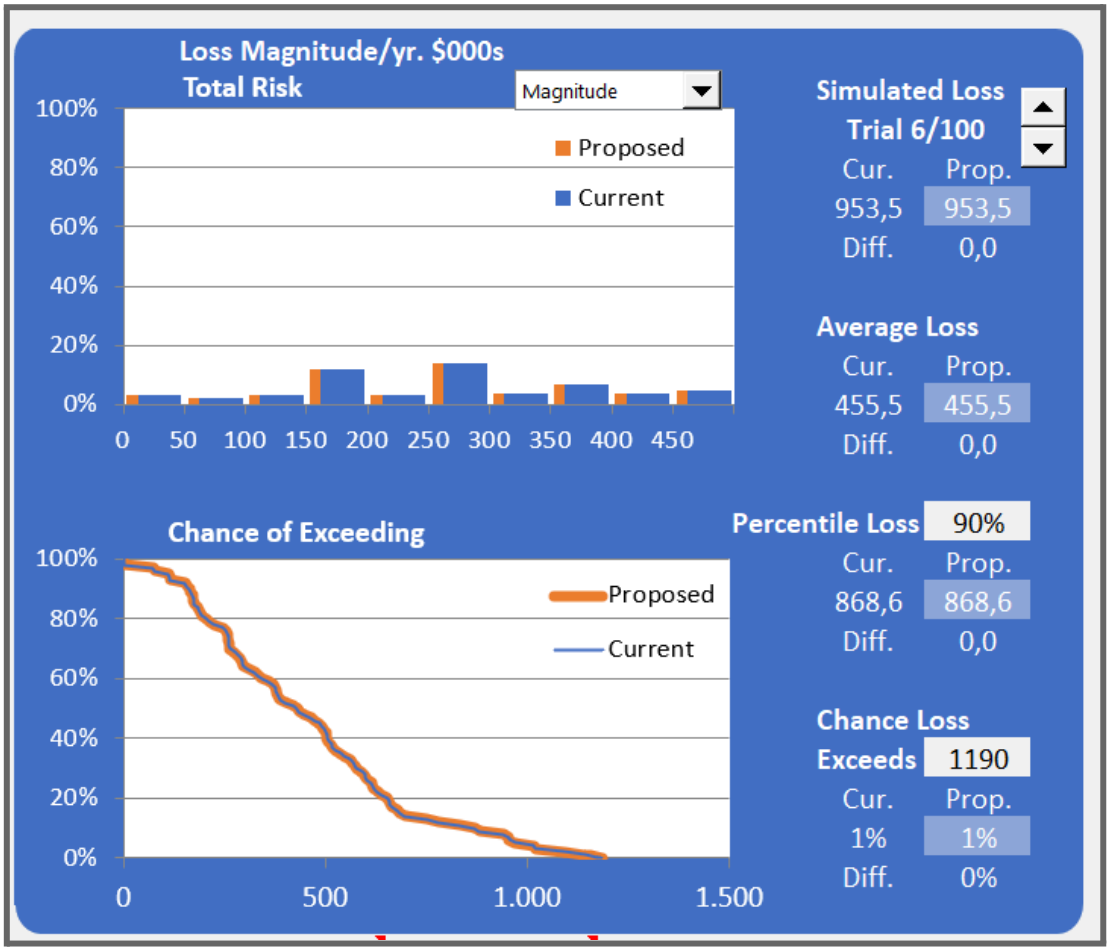
Secondary Loss Magnitude

SLEF	Min	ML	Max
Current	25%	35%	55%
Proposed			

Current	Min	ML	Max
Productivity			
Replacement			
Response	2	3	5
Reputation	3	5	8
Competitive Adv.	10	20	30
Judgments	2	4	7

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

ANÁLISIS COSTE ESTIMADO



CONCLUSIONES

- El coste medio que va a suponer para la empresa es de 455.500€ al año
- La probabilidad de que en un año este incidente genere pérdidas de más de 800.000€ es del 12%
- El coste máximo que la empresa puede asumir al año es de 1.190.000€.