Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 1

Sesión práctica 1:

CORAS.

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. PREPARACIÓN PARA EL ANÁLISIS

ChaseMyCash, una empresa emergente compuesta por 3 cofundadores y una plantilla de 18 empleados, logró generar ingresos por valor de 1.000.000 euros en el año 2022, con un EBITDA aproximado de 300.000 euros. Tienen como meta mejorar estas cifras para el año 2023.

ChaseMyCash ofrece a los usuarios la capacidad de gestionar sus finanzas personales o del hogar a través de una plataforma web y una aplicación móvil que actualmente se encuentra en desarrollo. La oferta de servicios incluye cuatro niveles de licencia, abarcando desde el resumen mensual de ingresos y gastos, hasta alertas personalizadas sobre los gastos, control de transacciones con tarjetas, gestión compartida de gastos, asesoramiento en inversión y ahorro, además de ofertas adaptadas de productos financieros y asesoramiento fiscal.

El proceso de registro se realiza en línea y requiere de detalles personales, laborales y financieros, junto con un historial bancario de los últimos seis meses. La plataforma utiliza un motor de inteligencia artificial para ofrecer recomendaciones personalizadas y consejos financieros.

Actualmente, cuentan con alrededor de 20.000 clientes en todo el mundo, principalmente usuarios domésticos. La empresa opera en un espacio de coworking y facilita el teletrabajo al 100% para su equipo. Proporcionan a sus empleados equipos completos, que incluyen ordenadores portátiles, teclados, ratones y monitores, y emplean servicios como AWS y GitHub para su infraestructura y repositorio de código, respectivamente. Utilizan aplicaciones de gestión y colaboración basadas en la nube, eliminando la necesidad de mantener servidores propios o adquirir licencias de software.

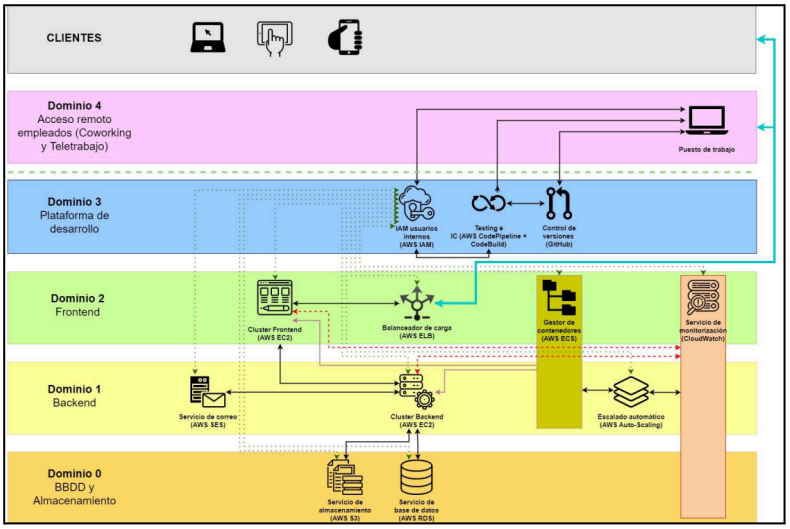
2. PRESENTACIÓN POR PARTE DEL CLIENTE DEL OBJETIVO DEL PROYECTO

El entorno en el que opera ChaseMyCash presenta un nivel elevado de preocupación debido a la falta de atención previa a este tema, y desean hacer de ello una prioridad inmediata. Para lograrlo, han contratado recientemente a dos individuos: uno para supervisar la seguridad empresarial y otro para asegurar la integridad de los productos. Su meta es que el equipo de seguridad continúe expandiéndose en el futuro, ajustándose a las necesidades detectadas. Todos los miembros del personal de la empresa estarán implicados en este proceso. El ámbito de acción está definido por las áreas de seguridad que buscan fortalecer (corporativa y de productos).

3. REDEFINICIÓN DEL OBJETIVO MEDIANTE DIAGRAMAS DE ACTIVOS

Se realizará un examen minucioso de los recursos y elementos clave dentro de la entidad para entender su funcionamiento e identificar las necesidades prioritarias. Con ello, conseguiremos enfocarnos en evitar situaciones críticas de manera eficaz. Para lograr este objetivo, se organizarán sesiones de trabajo con los integrantes del equipo y el cliente, con el fin de discutir y resolver cualquier interrogante que emerja.

Tal como se mencionó previamente con detalle, cada dominio está implicado de cierta forma. La configuración del sistema se extiende desde el dominio 4, permitiendo a los trabajadores el acceso remoto para el manejo y control de las herramientas pertenecientes al dominio 3, hasta el dominio 0. Este último engloba tanto los servicios de almacenaje como los de base de datos empleados por la aplicación.



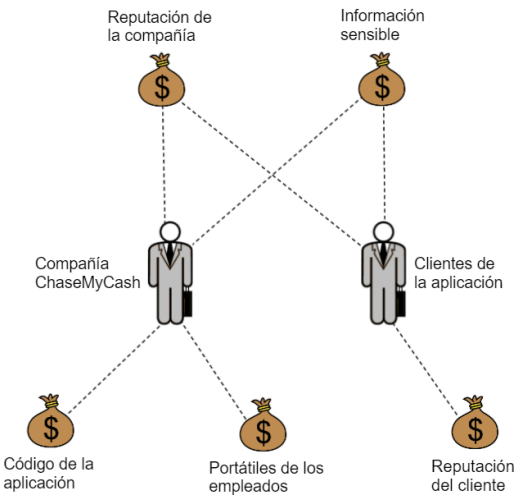
Identificación de los activos:

- Reputación de la compañía
- Imagen proporcionada a los clientes
- Información sensible de los usuarios
- Código fuente del software.

Las entidades afectadas en caso de que se produjera un cambio en los activos serían los siguientes:

- Los usuarios que hacen uso del servicio. (Clientes)
- La compañía ChaseMyCash. (Fundadores, empleados)

Diagrama de activos:



La compañía se verá afectada por los siguientes activos:

- Es conocido por todos que la **imagen corporativa** es un activo primordial para los fundadores y, en este caso, para el equipo de ChaseMyCash. Una percepción negativa puede afectar adversamente la lealtad de los clientes y, por ende, la viabilidad económica de la empresa. Mantener una reputación positiva es esencial para el crecimiento y la estabilidad a largo plazo de la empresa.

- **El código fuente del software** representa la esencia de la plataforma de ChaseMyCash. Es vital para los creadores y trabajadores de la compañía proteger este activo contra vulnerabilidades que podrían ser explotadas por actores maliciosos para acceder indebidamente a los sistemas y datos. La integridad y seguridad del código fuente son fundamentales para la operación y confiabilidad de la plataforma.

La clientes se verán afectada por los siguientes activos:

- La **percepción que tienen los clientes de ChaseMyCash** es de suma importancia para los directivos y el personal de la compañía, ya que una imagen negativa puede influir de manera adversa en la fidelidad de los clientes y, por consiguiente, en el desempeño económico del negocio.

- La **protección de la información personal** y confidencial de los usuarios es primordial para ChaseMyCash. Este activo es esencial para la confianza y seguridad de los clientes. Una gestión ineficaz, o una brecha de seguridad que comprometa estos datos, podría tener consecuencias devastadoras, no sólo en términos de pérdida de confianza y credibilidad entre los usuarios, sino también en posibles sanciones legales y financieras para la empresa. Es vital implementar medidas robustas de seguridad y privacidad para salvaguardar la información.

Lista de incidentes no deseados:

Tras realizar una serie de reuniones y debates con todo el equipo de análisis se obtiene el siguiente listado de incidentes no deseados.

		
¿Quién o qué es la causa?	**¿Cómo?, ¿Qué podría pasar?, ¿Qué es lo que puede ser dañado?**	**¿Qué hace posible esta situación?**
Hacker	Se podría producir una brecha de datos debido al acceso no autorizado por parte de un usuario con malas intenciones.	La configuración de los buckets del S3 es la predeterminada, por lo que los elementos almacenados no están cifrados.

Empleado	Un empleado podría eliminar, de manera accidentada, una tabla de la base de datos, provocando una pérdida de información o incluso, una denegación del servicio	Ausencia de política de copias de seguridad
Empleado	Un empleado podría, descargar de manera accidentada, un recurso malicioso, que comprometa los equipos de los empleados.	Ausencia de políticas de empresa que restrinjan la descarga de software de terceros.
Dispositivo de empleado	En caso de que alguno de estos dispositivos esté infectado con software malicioso, existe el riesgo de que dicho malware se propague a través de la red y ponga en peligro los sistemas y datos de la organización.	Empleo de dispositivos personales en el trabajo.

4. APROBACIÓN DEL OBJETIVO

En esta etapa, se busca obtener la aprobación del cliente y se definen los criterios que el analista utilizará en los siguientes pasos de la metodología, específicamente en relación con la probabilidad e impacto.

Las Tablas detallan los valores asignados a la probabilidad e impacto que serán utilizados para la estimación de riesgos durante el análisis. Basándose en estos niveles predefinidos, se genera la matriz de riesgos presentada en la última Tabla 6, la cual será empleada como referencia clave en las siguientes fases del proceso. El análisis se realizará sobre 4 tipos de riesgos concretos.

Escala de probabilidad para los 4 riesgos:

PROBABILIDADES		
1	**Raramente**	Ocurre como mucho una vez cada 2 años
2	**En ocasiones**	Ocurre como mucho una vez cada 1 año
3	**Regularmente**	Ocurre como mucho una vez cada 6 meses
4	**Frecuentemente**	Ocurre como mucho una vez cada 3 meses

Escalas de impacto:

ESCALA DE IMPACTO PARA LA BRECHA DE DATOS QUE AFECTA CÓDIGO DE LA APLICACIÓN		
1	Leve	Solo impacta a una fracción inferior al 1% de los datos de la aplicación y puede ser corregido en menos de un día.
2	Moderado	Impacta entre el 1% y el 10% de los datos sensibles de la aplicación y se puede solucionar en menos de una semana.
3	Grave	Impacta entre el 10% y el 50% de los datos sensibles de la aplicación y su corrección lleva más de un mes.
4	Catastrófico	Afecta a más del 50% de los datos de la aplicación y compromete la funcionalidad; solucionarlo lleva más de seis meses.

En la reunión, tanto el responsable de seguridad corporativa como el "CTO" coincidieron en que una brecha de datos que impacta en el código de la aplicación representa un riesgo significativo, dado que el producto de la empresa es un software. Ambos transmitieron al CEO y al COO la importancia de este riesgo, explicando que si se filtra todo el código o una parte de él, podría afectar negativamente al negocio. La razón es que cualquier otra empresa podría utilizar y distribuir el código de manera gratuita, lo que podría resultar en la pérdida de clientes que ya no estarían dispuestos a pagar por el producto.

ESCALA DE IMPACTO PARA RANSOMWARE		
1	Leve	Menos del 10% de los archivos de la empresa están encriptados y el tiempo de recuperación es inferior a un día
2	Moderado	Entre el 10% y el 50% de los archivos críticos de la empresa están encriptados y el tiempo de recuperación es inferior a una semana.
3	Grave	Más del 50% de los archivos críticos de la empresa están encriptados y se estima que el tiempo de recuperación es superior a un mes.
4	Catastrófico	La víctima pierde acceso a más del 90% de sus datos críticos, lo que resulta en la pérdida de contratos y la exposición de información confidencial.

En relación con este riesgo, el COO expresó una especial preocupación por la posibilidad de que el ransomware afectará a datos personales de los clientes, debido a las implicaciones legales que esto conlleva. Subrayó la necesidad de informar a las autoridades competentes en caso de que la brecha involucre datos personales.

Por su parte, al CEO le inquietaba la posible repercusión en la reputación de la empresa si se llegara al punto de tener que comunicar la infección por ransomware a las autoridades, ya que esto podría afectar la imagen de la empresa y resultar en la pérdida de clientes.

El CTO, por otro lado, mostró su preocupación porque el ransomware pudiera afectar a los equipos principales en los que se desarrolla el código, lo que resultaría en la imposibilidad de trabajar en el producto. Por lo tanto, lo que más preocupa en relación con el ransomware es su impacto potencial en datos personales o en las máquinas fundamentales para el desarrollo del producto de la empresa.

ESCALA DE IMPACTO PARA BRECHA DE DATOS DE CLIENTES		
1	Leve	Afecta a una pequeña cantidad de datos personales, como direcciones de correo electrónico o números de teléfono, sin evidencia de uso malicioso.
2	Moderado	Afecta a una cantidad significativa de datos personales, como nombres completos y direcciones postales, y puede existir alguna evidencia de uso malintencionado.
3	Grave	Afecta a una gran cantidad de datos personales con evidencia de uso malintencionado, como el robo de información de tarjetas de crédito o contraseñas de cuentas bancarias.
4	Catastrófico	Afecta a datos personales o financieros críticos, como números de seguridad social o información de cuentas bancarias.

Durante la reunión, el CTO manifestó inquietud acerca de las implicaciones directas de una brecha de datos de clientes en el producto, afectando su integridad y dirección futura. El desarrollador expresó su preocupación por la posibilidad de que la brecha de datos de clientes esté relacionada con vulnerabilidades en el código, mientras que el arquitecto en la nube compartió la misma preocupación, centrándose también en la seguridad del almacenamiento en la nube para datos personales.

Por otro lado, el responsable de seguridad resaltó la necesidad imperante de implementar tecnologías adecuadas y la importancia de contar con formación en DevSecOps. Su énfasis radicó en prevenir la ocurrencia de brechas de datos de clientes mediante enfoques y procesos seguros desde la etapa inicial del desarrollo.

ESCALA DE IMPACTO PARA DENEGACIÓN DE SERVICIO		
1	Leve	La denegación de servicio es temporal y no afecta significativamente la operación del sistema o servicio, con equipos sin disponibilidad durante días o horas.
2	Moderado	La denegación de servicio es prolongada y afecta a algunos servicios o aplicaciones críticas, lo que puede generar cierta interrupción en la operación del negocio, con equipos sin disponibilidad durante días o semanas.

3	Grave	La denegación de servicio es extensa y afecta a servicios o aplicaciones críticas, lo que provoca una interrupción significativa en la operación del negocio y puede tener consecuencias financieras, con equipos sin disponibilidad durante semanas o meses.
4	Catastrófico	La denegación de servicio es masiva y afecta a servicios o aplicaciones críticas en todo el sistema, lo que provoca una interrupción total de la operación del negocio y puede tener consecuencias financieras graves, con equipos sin disponibilidad durante meses o años.

El responsable de seguridad expresó inquietud acerca de la ausencia de implementación de metodologías de desarrollo seguro en las fases iniciales del proceso de desarrollo del producto. En el caso de una posible denegación de servicio provocada por una vulnerabilidad en el producto, el desarrollador mostró preocupación por la necesidad de abordar y corregir el problema. El CTO, por su parte, se preocupó por las repercusiones de la denegación de servicio en el producto, señalando que al tratarse de un producto de software, afectaría directamente a su disponibilidad, impidiendo que los clientes lo utilicen.

Por otro lado, el arquitecto en la nube expresó una preocupación particular en relación con este riesgo, ya que toda la infraestructura del producto está desplegada en AWS. En esta situación, la denegación de servicio podría originarse tanto por fallos o mala configuración en la arquitectura misma como por una interrupción en el servicio proporcionado por el proveedor de servicios en la nube, afectando así al producto.

Matriz de riesgo:

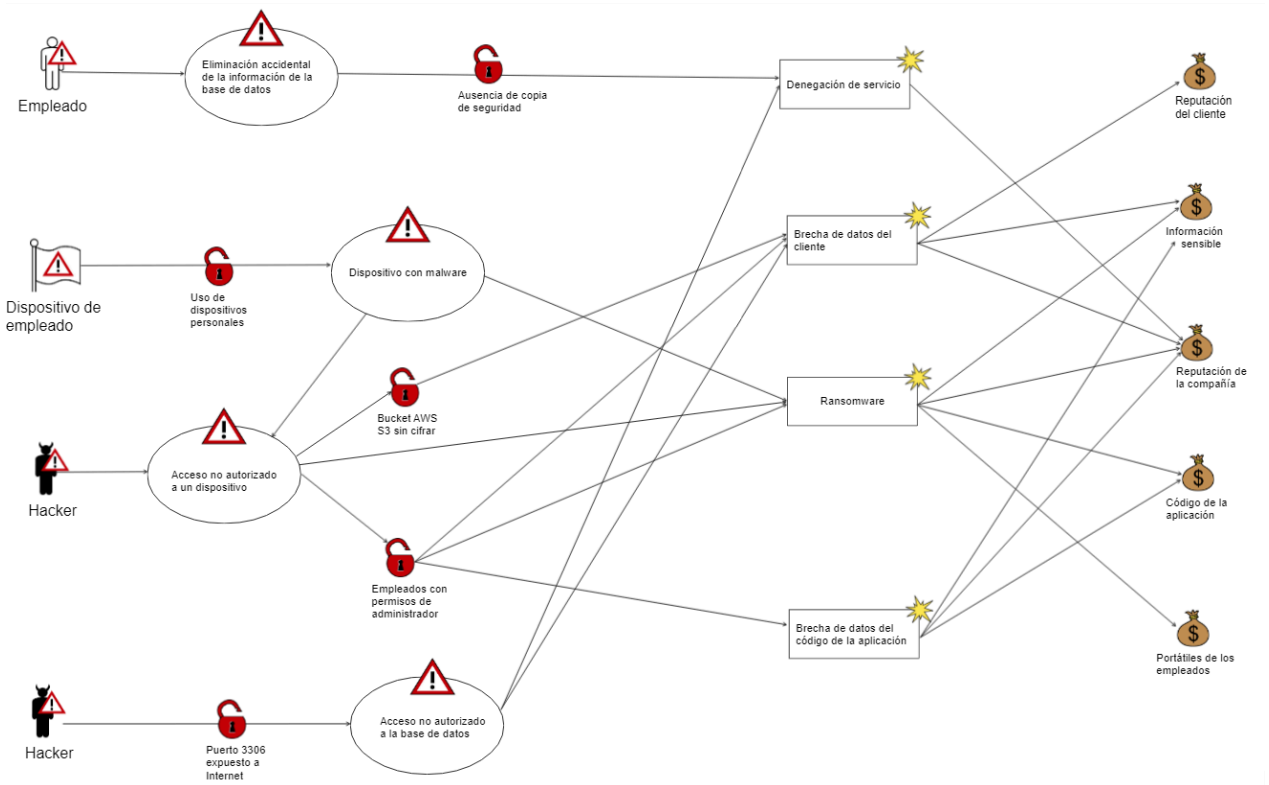
Una matriz de riesgo nos va a permitir identificar los posibles riesgos, clasificándolos en función de su probabilidad de ocurrencia y su impacto en el sistema. Con lo que podremos priorizar las acciones de mitigación, enfocándonos en aquellos riesgos que tienen el mayor impacto potencial en el sistema.

I / P	Raramente	En ocasiones	Regularmente	Frecuentemente
Leve				
Moderado				
Grave				
Catastrófico				

5. IDENTIFICACIÓN DE LOS RIESGOS MEDIANTE DIAGRAMAS DE AMENAZAS

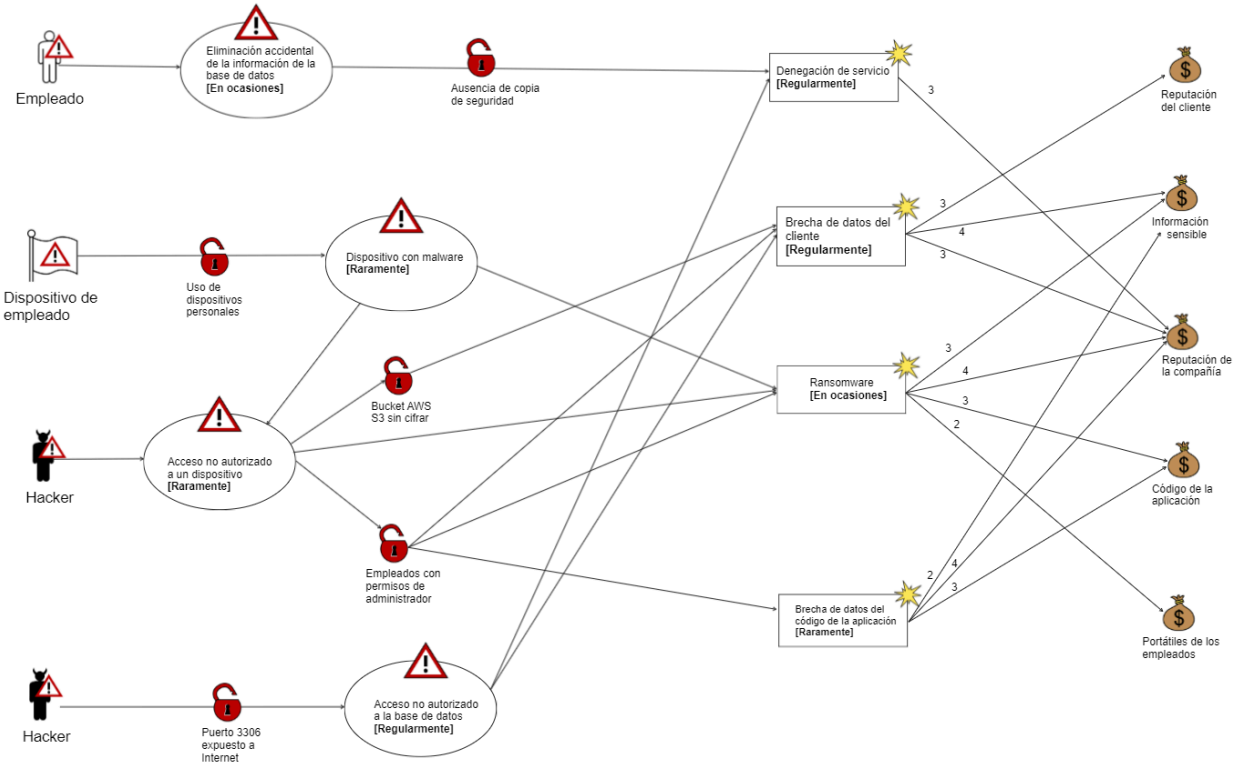
Una vez establecidos los riesgos y los niveles de probabilidad e impacto que se utilizarán, es esencial identificar cuándo y cómo podrían ocurrir mediante el modelado de amenazas, una práctica inherente a la metodología CORAS. La Figura 1 ilustra el modelo correspondiente a los riesgos de seguridad corporativa, mientras que la Figura 2 representa el asociado a los riesgos de seguridad del producto.

En la Figura 1, se identifican como amenazas a un empleado malicioso y a un cibercriminal. El primer incidente no deseado considerado es una brecha de datos del código de la aplicación, que afecta al producto como activo. Las vulnerabilidades que podrían provocar este incidente incluyen la falta de control de privilegios y permisos para los internos. En contraste, un cibercriminal podría aprovechar los puertos abiertos y la predisposición a ataques de phishing debido a la falta de concienciación en ciberseguridad entre los empleados. Estas debilidades permitirían a los atacantes acceder al repositorio de GitHub y modificar o eliminar el código del producto.



6. ESTIMACIÓN O VALORACIÓN DEL RIESGO

Utilizando el diagrama anterior como base, se asignarán unas probabilidades y unos impactos, con la finalidad de estimar el riesgo acorde a las escalas definidas anteriormente.



7. EVALUACIÓN DEL RIESGO

Una vez asignadas las probabilidades y los impactos ya podemos rellenar la matriz de riesgos, en ella se analizaron qué riesgos son asumibles y cuáles no para ChaseMyCash.

I / P	Raramente	En ocasiones	Regularmente	Frecuentemente
Bajo				
Moderado				
Grave	Brecha de datos del código	Ransomware	Denegación de servicio	
Catastrófico			Brechas de datos de clientes