Análisis y gestión del riesgo

Práctica 2: Gestión de riesgos en ChaseMyCash

Marta Beltrán Pardo

Contenidos

1. Introducción

Para la realización de esta práctica los miembros del equipo siempre adoptarán los roles de responsables de seguridad corporativa y de producto.

En total realizaremos 2 sesiones en el aula relacionadas con esta práctica, las fechas se indicarán con antelación suficiente en el calendario de la asignatura en Aula Virtual.

Al final de esta práctica habréis decidido cómo gestionar, inicialmente, los riesgos para la empresa ChaseMyCash que habéis evaluado a lo largo de la práctica 1.

2. Material para la realización del caso

A continuación, se enumeran los materiales necesarios para la realización de esta práctica, que pueden descargarse desde el Aula Virtual:

- **Práctica2_Guion.pdf**: este documento.
- **Dossier ChaseMyCash.pdf**: información sobre la empresa con la que vamos a trabajar en los casos y las prácticas.
- **Resultados obtenidos en la práctica 1.**
- **Recomendaciones y mejores prácticas recogidos en documentación como el NIST Cybersecurity Framework, el OWASP ASVS ó el Security Guidance de la CSA.**

3. Normativa y evaluación

En este apartado se detalla el formato de entrega de la práctica y la forma en la que se evaluará la misma:

- El porcentaje de la nota final de la asignatura al que corresponde esta práctica puede consultarse en la Guía docente de la propia asignatura.
- El caso deberá realizarse, de forma obligatoria en el aula los días indicados en el calendario de la asignatura en Aula Virtual, en grupos de cuatro personas. Para la asignación de los grupos se deberán seguir las indicaciones del profesor. Será necesario trabajar fuera del aula para terminar las tareas propuestas.
- Cada grupo deberá entregar una única copia de la memoria (entregables de las sesiones) a través de Aula Virtual. La fecha límite para cada entrega se avisará con tiempo suficiente.
- Los entregables deben ser, como mínimo, los propuestos en el siguiente apartado.

4. Enunciado de la práctica

Como ya se ha comentado en el apartado de Introducción, en esta práctica vais a realizar un proceso de gestión de riesgos, proponiendo para ello diferentes planes que permitan escoger la mejor estrategia para gestionar cada riesgo y desplegarla en el corto/medio plazo.

Para ello se proponen las siguientes tareas y entregables asociados a cada una de las sesiones de trabajo. Los entregables tienen que generarse de manera profesional, como se haría en un proceso de gestión de riesgos real.

SESIÓN 1 – Gestión de riesgos: trabajo inicial

En esta sesión se esbozará un Programa de Ciberseguridad. Para ello se trabajará con la estructura estudiada en la unidad 9 de la asignatura. Es decir, se propondrá:

- La arquitectura de referencia de seguridad para ChaseMyCash con las capacidades de seguridad que se consideren necesarias para gestionar los riesgos evaluados con las estrategias más adecuadas (centrándose en la mitigación).
- Propuesta de controles, contramedidas y herramientas que permitan desplegar estas capacidades. Matriz de cobertura de las capacidades.
- Políticas de seguridad que habría que comenzar a aplicar de manera prioritaria (basta con hacer un listado).
- Recursos humanos necesarios (nuevos o ya existentes) para llevar a cabo este plan.

Entregable 1 – Primera versión del Programa de Ciberseguridad de ChaseMyCash teniendo en cuenta los riesgos evaluados durante la práctica 1.

SESIÓN 2 – Gestión de riesgos: planes directores/de acción

En esta sesión nos centraremos en los planes de mitigación, desde el punto de vista de la seguridad y de la protección de datos.

El objetivo es planificar el trabajo para los siguientes 12 meses (primer plan director) y saber qué se puede esperar en cuanto a reducción del ciberriesgo. Para ello se compararán los riesgos inherentes cuantificados en la práctica 1 con los residuales (post-mitigación) que se esperan observar pasados 12 meses.

Entregable 2 – Plan director de seguridad para mitigar los riesgos de seguridad en los que en la primera sesión se haya escogido la estrategia de mitigación. Debe recoger los proyectos que se realizarán en los primeros 12 meses (descripción, tareas, responsables, temporización, recursos necesarios – no es imprescindible un presupuesto-). También se debe incorporar una evaluación de riesgo con FAIR que compare el riesgo antes de mitigación con el riesgo después de mitigación, de manera que se comprendan los beneficios que se espera obtener.

Entregable 3 – Plan de acción asociado a la evaluación de impacto para la protección de datos (sesión 5 de la práctica 1). De nuevo debe incluir una comparación del riesgo inicial o inherente con el residual para que se comprendan los beneficios que se espera obtener con este plan.