**Análisis de riesgo**

**Resumen del proceso**

Como primer paso, ya teniendo definido el alcance y los activos de TI relevantes para el caso de análisis, deberíamos verificar cuales son las posibles amenazas que podrían comprometer estos activos, y en estos casos particulares (Fuga de información, modificación no autorizada de información y denegación de servicio) lograr profundizar más en detalle qué eventos pueden causar estos problemas.

Luego sería necesario identificar los puntos débiles de los sistemas, en conjunto de las medidas de seguridad que se están manteniendo en práctica (Como la certificación PCI DSS en este caso), para tener un panorama del estado de situación en el cual se debe realizar el análisis de riesgos.

Una vez realizado el análisis anteriormente mencionado, llegaría el momento de realizar la evaluación de riesgo, donde se determinará en medidas cualitativas o cuantitativas la posibilidad de que los riesgos se materialicen.

Para determinar el nivel de riesgo teniendo en cuenta un análisis cualitativo, se tienen en cuenta las variables de impacto y probabilidad.

Por último, se determinarán que riesgos se asumirán y que riesgos se deberán mitigar, indicando qué métodos se pueden utilizar para cubrirlos.

Abordando el caso planteado, separaré el análisis para cada problema planteado:

**Fuga de información.**

Si bien Seguridad Informática no posee conocimiento de qué dato será almacenado en cada base de datos, es clave poder clasificar la información para así poder determinar las medidas necesarias para resguardarla.

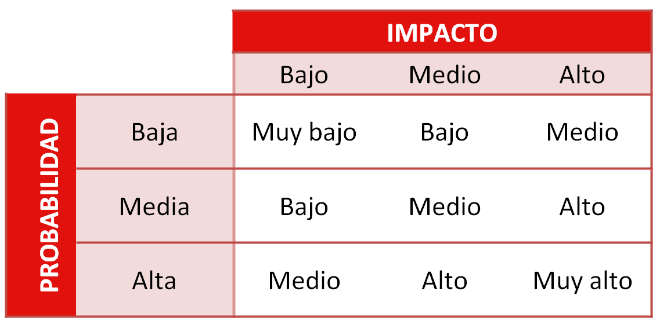
A continuación abordaremos cuales podrían ser algunas causas de fuga de información:

* Accesos no autorizados a las aplicaciones
* Accesos no autorizados a las bases de datos
* Intercepción de información que no viaje encriptada
* Interfaces de seguridad débil (Por ejemplo, donde se utilice un repositorio intermedio no seguro) o interfaces manuales
* Poco control de la información ante la desvinculación de un empleado (Se estima que más del 59% de las desvinculaciones se lleva consigo información de la compañía donde trabaja, lo que siempre genera un riesgo alto de pérdida de la misma.
* Poco control en la seguridad de la información que se maneja con proveedores
* Poco control en los dispositivos que utilizan los empleados de la empresa
* Falta de seguridad en la robustez de las contraseñas generando contraseñas fáciles de descifrar
* Poco control de información física (Por ejemplo, documentación suelta en las oficinas o desatendida en la fotocopiadora)
* Poca concientización a los empleados sobre el riesgo de pérdida de información

*Nota: Se presupone que debido a la certificación PSI DSS los firewall y antivirus se mantienen actualizados manteniendo una red segura y se realizan controles de vulnerabilidad, por lo que se obvian riesgos bajos como la posibilidad de que un malware comprometa la información.*

Si bien Mercado Libre cuenta con la certificación PSI DSS que valida la seguridad de los datos de las tarjetas, se considera que dada la cantidad de factores que pueden provocar la fuga de información, teniendo en cuenta un dato no menor y no controlable al 100%, que es el factor humano que puede cometer errores que generen la fuga de información, y que en años anteriores hubo récord histórico de fuga de datos en empresas, el riesgo de fuga de información se determina como **ALTO**.

Para definir dicha calificación, se utilizó el siguiente estándar de comparación entre el impacto y la probabilidad de que el riesgo se materialice:



Teniendo en cuenta un impacto **Alto** y una probabilidad **media**.

La valoración del impacto se determinó teniendo en cuenta la cantidad de factores que pueden afectar a los activos de TI y a la gran cantidad de posibles errores que generen la fuga de información.

La valoración de la probabilidad, fue determinada teniendo en cuenta que Mercado Libre no es una pequeña empresa sino que tiene sumamente desarrollada la actividad de seguridad de la información y el control interno de la compañía.

**Modificación no autorizada de información**

Las modificaciones no autorizadas pueden darse a nivel base de datos, ya sea modificando tablas o directo en los datos, o a nivel aplicación si la misma permite realizar este tipo de modificaciones.

A continuación se presentarán posibles causas de modificaciones no autorizadas:

* No existe una correcta asignación de accesos a nivel aplicación o base de datos (Accesos a tablas o datos no gestionados de manera correcta)
* En caso de existir usuarios genéricos con accesos de modificación, falta de monitoreo de la actividad de los mismos o de resguardo de su clave.
* Inadecuada segregación de funciones que permita realizar pasajes a producción no autorizados
* Falta de monitoreo y resguardo de los usuarios con altos privilegios que puedan realizar tareas pertinentes que puedan afectar a la modificación de información
* Inadecuada de separación de ambientes que permitan segregar las tareas de desarrollo, QA y producción
* Falta de una política o metodología de cambios que determine los pasos a seguir en cada cambio (Determinando que deben existir aprobaciones para realizar los cambios ya sea validando que el cambio
* Falta de seguridad en los repositorios de GitHub

*Nota: teniendo en cuenta que MercadoLibre es una empresa de tecnología con larga trayectoria, se tiene en cuenta un control interno desarrollado que realice análisis sobre los problemas planteados anteriormente, y una correcta metodología de administración de accesos por parte de seguridad informática.*

*Adicionalmente se presupone un proceso de cambios a programas sumamente desarrollado teniendo en cuenta las problemáticas anteriores.*

Dicho esto, se considera que el riesgo de modificaciones no autorizadas en la información es **MEDIO**, teniendo cuenta un impacto alto y una probabilidad baja.

**Denegación de servicio**

La denegación de servicios puede afectar directamente a la operatoria diaria de Mercado Libre desencadenando diversos problemas de performance en las plataformas.

Debido a que MercadoLibre es una compañía de gran tamaño que continúa en expansión, es muy probable que sea foco de diversos ataques, como puede ser un ataque DoS, ya sea proveniente de la competencia o de usuarios malintencionados.

Teniendo en cuenta la importancia y relevancia de Mercado Libre en el mercado hoy en día, podemos suponer que las probabilidades de que ocurran estos ataques son muy altas.

El impacto de la denegación de servicios clave, podría llevar al colapso de los servidores, por lo que el impacto sería **alto**.

Dadas estas razones, y debido a que los ataques DoS son muchas veces difíciles detectar, se define la criticidad del riesgo como **MUY ALTA**.

Presentación Ejecutiva

**Análisis de riesgo**

Se presenta a continuación el detalle sobre el análisis de riesgo realizado sobre tres eventos que se consideran críticos para la compañía.

**Fuga de información:**

La información es uno de los principales activos de Mercado Libre, la fuga de la misma podría generar las siguientes consecuencias:

* Daño a la imagen de la empresa
* Consecuencias Legales
* Consecuencias Económicas
* Suspensión de operaciones
* Problemas al realizar certificaciones de seguridad.

Debido a las graves consecuencias y que recientemente se han reportado daños por fuga de información en grandes empresas como Facebook, Linkedin, Zoom, se considera al riesgo de fuga de información con una criticidad **ALTA**.

**Formas de prevenirla:**

* Reforzar políticas de seguridad
* Capacitar a toda la compañía en dicha temática
* Generar una cultura laboral adaptada al riesgo
* Refuerzo en controles sobre proveedores

**Modificación no autorizada de información**

Las modificaciones no autorizadas a la información pueden generar pérdida de credibilidad sobre la información utilizada por Mercado Libre, se corre el riesgo de no poder validad completitud, integridad y exactitud de la información.

**Formas de prevenirla:**

* Refuerzo en políticas de seguridad de accesos
* Implementación de matriz de segregación de funciones
* Refuerzo en política de cambios en aplicaciones y en datos

**Denegación de servicio**

La denegación de servicios al igual que la fuga de información, son eventos clave donde el equipo de Seguridad Informática debe hacer foco para prevenirlo.

Un ataque de denegación de servicios puede generar la interrupción de la actividad de la empresa.

**Efectos**:

* Inactividad en el sitio web
* Caídas de servidores
* Perdidas de tiempo y dinero

**Formas de prevenirlo:**

* Actualización y mantenimiento constante de firewalls
* Implementación de sistemas de prevención de intrusos
* Constantes pruebas y controles para prevenir vulnerabilidades