Supuestos identificados:

1. Definir y documentar el plan de trabajo de las tres personas para el levantamiento de información del servicio que prestan los 7000 proveedores (contra el tiempo de levantamiento de información). Reunirse con el área de compras o el área encargada de la administración técnica de los contratos para identificar el objeto de los contratos, adicionalmente enviar por correo electrónico una proforma fácil de contestar preguntando sobre el objeto de contrato, servicio, tipo de servicio, entre otros para que podamos tener otro insumo por parte del proveedor.
2. Definir controles periódicos para revisar y realizar cambios pertinentes a la evaluación realizada por el área de Gestión de riesgos asegurando que se tengan definidos activos, accesos, información consultada, riesgos y vulnerabilidades.

**Problema 1**

OBJETIVOS

Desarrolla los criterios necesarios para segmentar y clasificar a los proveedores en función de su criticidad.

1. ¿Qué variables tendrías en cuenta para identificar a un tercero como crítico para Seguridad Informática?

**Propuesta:**

Primero se definen en compañía del negocio aquellas variables de negocio teniendo en cuenta las líneas de servicio de los proveedores, la estrategia de negocio de MELI y objetivos estratégicos de MELI, para que sea la compañía quien nos brinde estas variables y aspectos relevantes a tener en cuenta.

Por otra parte, nos apoyamos en el área legal para identificar la regulación de cada uno de los 18 países en los cuales MELI cuenta con representación y cuales proveedores se pueden segmentar en estas regionales de manera que tengamos variables regulatorias como multas, impacto reputacional, sanciones que puede acarrear MercadoLibre.

Por último, apoyándonos en los estándares y buenas prácticas podemos realizar la clasificación de los proveedores en dominios dando alcance a las siguientes variables:

Variables de seguridad de la información:

1. Gestión de accesos
2. Gestión de riesgos de terceras partes
   1. Controles de código malicioso
   2. Ramsonware
   3. Controles de red
3. Gestión y clasificación de activos
4. Clasificación de la información
5. Seguridad física y del entorno
6. Supply chain: como interviene el proveedor en la cadena del producto de MELI
7. Control operacional:
   1. Training
   2. Incidentes
   3. Plan de respuestas
   4. Plan de recuperación
   5. Gestión de cuartas partes
8. ¿Con qué criterio los clasificarías para determinar el nivel de criticidad de los proveedores?

**Propuesta:**

Medición de cada una de las variables

* 1. Realizar un análisis e identificación de riesgos de los procesos para cada uno de los siguientes ambientes:
     + Ciberseguridad
     + Cumplimiento
     + Estratégicos
     + Reputacionales
     + Operacionales
     + Financieros
  2. Adicionalmente, analizar y clasificar los riesgos de manera cuantitativa de manera que me permita identificar la relación de costos de los controles a implementar y la manera cualitativa es ponderar que puede llegar a ocurrir si un riesgo se materializa. Por ejemplo:
     + Valor y tamaño de contratos
     + Líneas base de solvencia financiera
     + Rating de seguridad de IT
     + Beneficiarios del negocio de las terceras partes
  3. El análisis y clasificación de manera cualitativa
     + Clasificación del tipo de servicio del proveedor
     + El acceso a los datos que necesitan de MELI
     + Categorización de la naturaleza de los datos por riesgo, por ejemplo, confidencialidad de la data, contraseñas
     + Expectativas acerca de la seguridad de la información

De acuerdo con las variables definidas y la clasificación de los proveedores, uno de los objetivos que quiero conseguir es que podamos cuantificar el porcentaje de cumplimiento sobre cada uno de los pilares de seguridad de la información, Confidencialidad, Integridad y Disponibilidad.

1. Detalla, bajo qué estándares o frameworks de seguridad realizarás la definición de las variables y criterios de los dos puntos anteriores.
   * NIST
   * COSO
   * ISO 27001
   * SOC 2

2. De aquellos proveedores identificados como críticos:

1. ¿Cómo realizarías el assessment de seguridad del Servicio?
2. ¿Qué preguntas y dominios incluirías en la evaluación del servicio?

El objetivo es evaluar cómo se encuentran los proveedores frente a los riesgos de ciberseguridad. Por lo anterior, el assessment lo haría dando alcance a los siguientes ambientes, calificando cada uno de los ambientes:

* + Gestión del ciclo de vida del producto
  + Gestión de seguridad del producto
  + Segregación de ambientes
  + Prevención de exploits
  + Actualizaciones de seguridad y firmado de software
  + Hardware root y booteo seguro
  + Testeo de seguridad
  + Gestión y configuración de seguridad
  + Gestión de vulnerabilidades

1. ¿Qué estrategia utilizarías para poder evaluar la mayor cantidad de proveedores en el menor tiempo posible?
   1. Primero: Una vez identificados y segmentados los proveedores por servicios, criticidad, etc. Defino unas plantillas proforma donde permita registrar, por parte nuestra y del proveedor las calificaciones de riesgos y controles con el fin que me permita tabular la información y desarrollando scripts con Python o Rstudio importaría estas proformas y las dejaría en un repositorio de información y la visualización de los aspectos que quiera ir validando.

3. Teniendo en cuenta el front-end del sistema (diseño de una pantalla):

1. ¿Cómo disponibilizamos la información para que las áreas interesadas den seguimiento a la gestión de terceros?
   * A corto plazo, plantearía implementar dos escenarios:
     + Si tenemos un archivo para el manejo de la información de los proveedores, lo haría a través de un sharepoint que permita gestionar los accesos a las partes interesadas y a los terceros correspondientes.
     + Por otra parte, si tenemos una aplicación desarrollada in house, podemos dar accesos en un servidor dedicado para tal aplicación.
   * A largo mediano plazo, defino procedimientos y lineamientos para la gestión de roles y perfiles más los accesos que deben tener las personas involucradas en el proceso de gestión de terceras partes.
2. ¿Cómo lo disponibilizamos a aquellos terceros que no contesten la evaluación, y cómo darías visibilidad a la Compañía sobre los riesgos que representan?

* Validaría con el área legal si se pueden realizar otrosíes o anexos a los contratos definiendo que sea de obligatoriedad.
* La visibilidad a la compañía dentro del comité de riesgos y de seguridad expondría los incumplimientos, sanciones, riesgos materializados en el sector.

1. Creando un modelo de riesgo
   * 1. Identificar los activos y datos confidenciales que almacenan, administran y gestionan.
     2. Creación del perfil de riesgo; riesgos potenciales asociados a activos individuales
     3. Priorización de activos; facilita la recuperación de sus procesos empresariales cuando se produce un evento inesperado
     4. Plan de mitigación; La segmentación de la infraestructura de TI, las políticas de copias de seguridad, la recuperación de desastres y los planes de continuidad
     5. Prevención de riesgos de vulnerabilidad y ciberseguridad;
     6. Monitoreo Constante
     7. Segmentación de ambientes, pruebas, producción y desarrollo

**Problema 2:**

Eres el responsable de evaluar la seguridad de los servicios de los terceros externos con los que MELI colabora. Tu tarea es evaluar el nivel de riesgo de seguridad de la información asociado a ese tercero y proponer un plan de acción para abordar los riesgos identificados.

Se ha evaluado un tercero con las siguientes características:

* Sirve como procesador de pagos en linea que utiliza Mercado Pago como pasarela de Pagos
* Tiene conexión P2P para compartir la información de conciliación de Pagos a través de SFTP
* La conexión es a través de VPN

Situaciones identificadas

* El tercero no tiene herramienta de DLP
* No tiene separación lógica de ambientes de la información de Mercado Pago respecto de otros clientes

Objetivo

1. Considerando el servicio y las situaciones identificadas, ¿qué planes de acción solicitaría al tercero para mejorar el servicio y seguridad de la conexión?
2. ¿Qué acciones complementarias/compensatorias planteamos para garantizar la seguridad de los datos de MELI mientras ejecutan el plan de acción?

Bonus

* En caso de que se identifique el que Tercero tuvo un incidente de tipo ransomware y no se conoce el impacto que pueda tener el servicio con Mercado Libre. ¿Cuáles son las acciones prioritarias que pediría al equipo de IT&Producto que accionara para tratar el incidente dentro de MELI? ¿Qué le solicitamos al tercero?