Caso - Sistema de riesgos TPRM

Contexto

Mercado Libre cuenta con un inventario de más de 10.000 proveedores que ofrecen distintos tipos de servicios a la organización.

Estos proveedores para poder brindar los servicios contratados, cuentan con distintos accesos a los sistemas, la infraestructura y por ende, a la información de Meli.

Dichos proveedores deben ser evaluados por el equipo de Gestión de Riesgos de Seguridad de Terceras Partes para acotar los riesgos y así garantizar que los mismos cumplen con los requisitos acordados, los niveles de seguridad necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información a la que acceden y por lo tanto que no exponen a Meli a potenciales riesgos de seguridad.

Supuestos

- El equipo de Gestión de Riesgos de Terceras partes de Seguridad se encuentra actualmente conformado por tres personas.
- Seguridad Informática en principio desconoce el servicio que ofrece el proveedor y el área de Meli que realiza la contratación.
    - En una segunda instancia, podría obtener los datos del servicio. Actualmente, se conoce el servicio de 1.000 proveedores.
- El flujo de interacción actual de Seguridad es con el área de Legales que se encarga puntualmente de los contratos.
- No se conoce el 100% de los flujos de sistemas por los que pasan los proveedores.
- Se tiene automatizado el envío de assessments y se concentran las métricas en un site.
- Del total de 10.000 proveedores tenemos la siguiente categorización:
    - 15% de proveedores identificados como críticos para Seguridad
    - 70% de proveedores sin identificación, lo que representa también un riesgo
    - 15% de proveedores no críticos para Seguridad.

Problema

Dado el volumen de assessment de terceros que debe realizar, el equipo de Gestión de Riesgos de Terceras Partes de Seguridad (TPRM Seguridad) debe realizar una sistema generalizado que abarque el envío automatizado de los assessments, concentre las métricas y divida el acceso por los diferentes usuarios (TPRM Seguridad, Tercero, otras áreas que quieran consumir información) con manejo de roles y perfiles.

Objetivo

1. Teniendo en cuenta el front-end del sistema (diseño de una pantalla):
    a. ¿Como disponibilizarías la información para que el proveedor conteste el assessment?
    b. ¿Como disponibilizarías aquellos terceros que no contesten el assessment, y como daría visibilidad a la Compañía sobre los riesgos que representan?
2. ¿Qué estrategia utilizaría para crear a los usuarios en el sistema según su rol y cuanto tiempo debería tener de validez el usuario (en el caso de los terceros)?

Bonus

1. ¿Cómo harías un primer borrador del front que va a visualizar el tercero? Botones, opciones, visualización, etc.
2. ¿Qué herramientas utilizarías para hacer búsquedas inteligentes en la base de datos de proveedores, sino conocemos el nombre exacto del tercero?