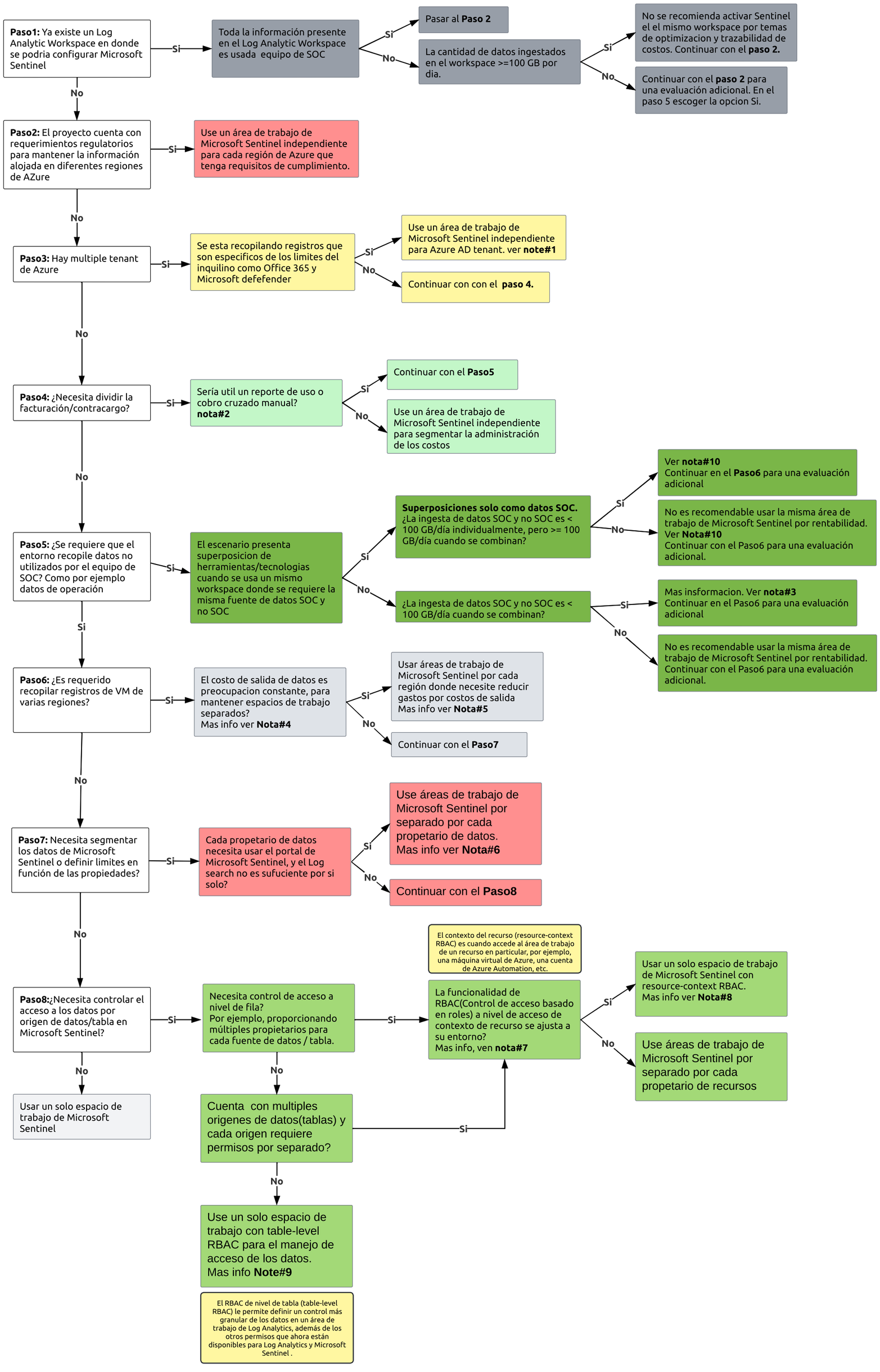
Diseño de la arquitectura de áreas de trabajo de Microsoft Sentinel



Nota#1: Los registros específicos con limites en un solo inquilino, como los de Office 365 y Microsoft Defender for Cloud, solo se pueden almacenar en el área de trabajo dentro del mismo inquilino.

Aunque es posible usar recopiladores personalizados para recopilar registros específicos de inquilinos de un área de trabajo de otro inquilino, no se recomienda hacerlo debido a las siguientes desventajas:

- Los datos recopilados por conectores personalizados se ingieren en tablas personalizadas. Por lo tanto, no podrá usar todas las reglas y libros integrados.
- Algunas de las características integradas, como UEBA (Análisis de comportamiento de eventos) y las reglas de aprendizaje automático, no tienen en cuenta las tablas personalizadas.
- Los conectores personalizados requieren un coste y esfuerzo adicionales, como el uso de Azure Functions y Logic Apps.
- Si estas desventajas no suponen ningún problema para la organización, vaya al paso 4 en lugar de usar áreas de trabajo de Microsoft Sentinel independientes.

Nota#2: Para obtener más información, vea Costos y facturación de Microsoft Sentinel. https://learn.microsoft.com/es-es/azure/sentinel/billing

Nota#3: Aunque generalmente se recomienda que los clientes tengan un área de trabajo independiente para los datos que no sean SOC, de modo que estos datos no acarreen costos de Microsoft Sentinel, puede haber situaciones en las que combinar datos SOC y datos que no sean SOC resulte menos costoso que separarlos.

Por ejemplo, considere una organización que tenga registros de seguridad que ingieran 50 GB/día, registros de operaciones que ingieran 50 GB/día y un área de trabajo en la región Este de EE. UU. https://learn.microsoft.com/es-es/azure/sentinel/billing

Nota#4: La salida de datos hace referencia al coste de ancho de banda por mover datos fuera de centros de datos de Azure.

Nota#5: Se recomienda tener el menor número de áreas de trabajo posible. Use la calculadora de precios de Azure para calcular el coste y determinar qué regiones necesita realmente, y combine las áreas de trabajo de regiones con costes de salida https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Nota#6: Para acceder al portal de Microsoft Sentinel hace falta que cada usuario tenga al menos un rol Lector de Microsoft Sentinel, con permisos de Lector en todas las tablas del área de trabajo. https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Nota#7: Con el fin de configurar RBAC de contexto de recursos para recursos que no sean de Azure, puede que le interese asociar un identificador de recurso a los datos al enviarlos a Microsoft Sentinel, de modo que el ámbito del permiso se pueda establecer mediante RBAC de contexto de recursos. https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Nota#8: Con los permisos de recursos o el contexto de recursos los usuarios pueden ver registros únicamente de los recursos a los que tengan acceso. El modo de acceso al área de trabajo debe establecerse en Permisos de recurso de usuario o área de trabajo. https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Nota#9: Con RBAC de nivel de tabla puede definir un control más pormenorizado de los datos de un área de trabajo de Log Analytics, así como los demás permisos. https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Nota#10: Se recomienda usar un área de trabajo independiente para los datos que no sean SOC, de modo que estos datos no acarreen costos de Microsoft Sentinel. https://learn.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree