Para Solucionar las problemáticas vistas dentro del laboratorio de ciberseguridad es necesario tomar en cuenta los siguientes puntos:

- **Recopilación de paquetes de red:** Se debe implementar un sistema de captura de paquetes de red en un punto de acceso estratégico, como un switch o un router, que permita interceptar el tráfico entre el departamento de Recursos Humanos y el departamento de Ventas.

- **Almacenamiento y procesamiento de datos:** Los paquetes capturados deben almacenarse en una base de datos adecuada para su posterior análisis. Se puede utilizar una base de datos relacional o no relacional, según las necesidades y el rendimiento requerido. Además, se debe implementar un sistema de procesamiento en tiempo real para realizar un análisis continuo de los paquetes capturados.

- **Análisis de patrones:** Utilizando técnicas de análisis de datos y aprendizaje automático, se debe construir un modelo de reconocimiento de patrones que pueda identificar anomalías de seguridad en los paquetes de red. Esto implica entrenar el modelo con datos históricos y etiquetados, donde se identifiquen los patrones normales y las anomalías conocidas.

- **Implementación de reglas de seguridad:** Una vez que se ha identificado una anomalía, se deben definir reglas de seguridad para tomar medidas adecuadas. Estas reglas pueden incluir la generación de alertas, el bloqueo de ciertos tipos de tráfico o la notificación a los equipos de seguridad de la empresa.

- **Capacitar al personal a seguir medidas de seguridad:** No solamente se debe depender del software para cubrir fallas o brechas de seguridad, dado que el mayor factor de error es el humano y es el más impredecible. Por lo tanto es importante capacitar al personal con medidas de seguridad eficientes. Desde no almacenar claves o datos de usuario dentro de sus equipos hasta limitar los sitios a visitar, además de las descargas.

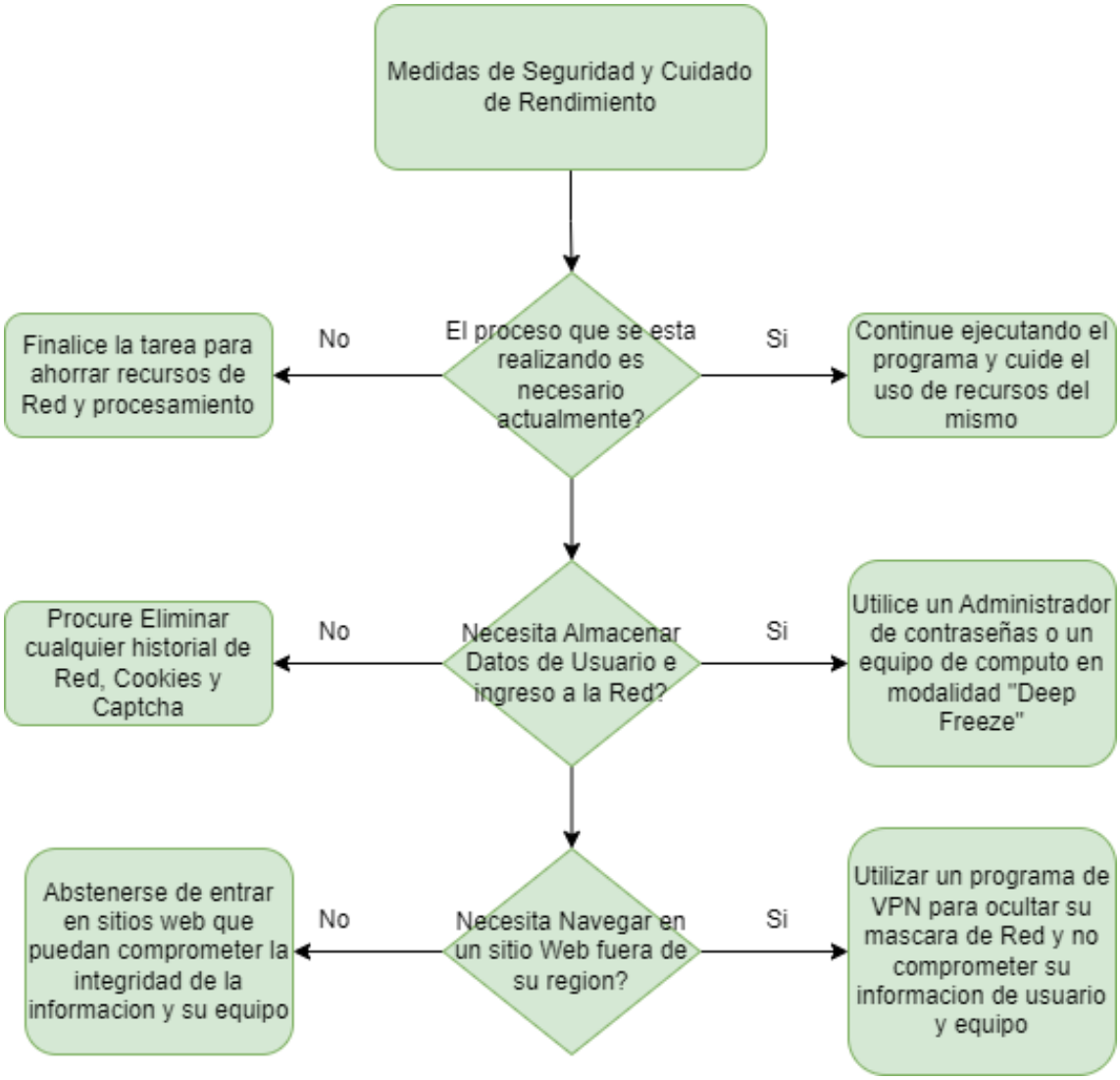
En cuanto a los factores de rendimiento y tiempo de desarrollo, se deben tener en cuenta los siguientes aspectos:

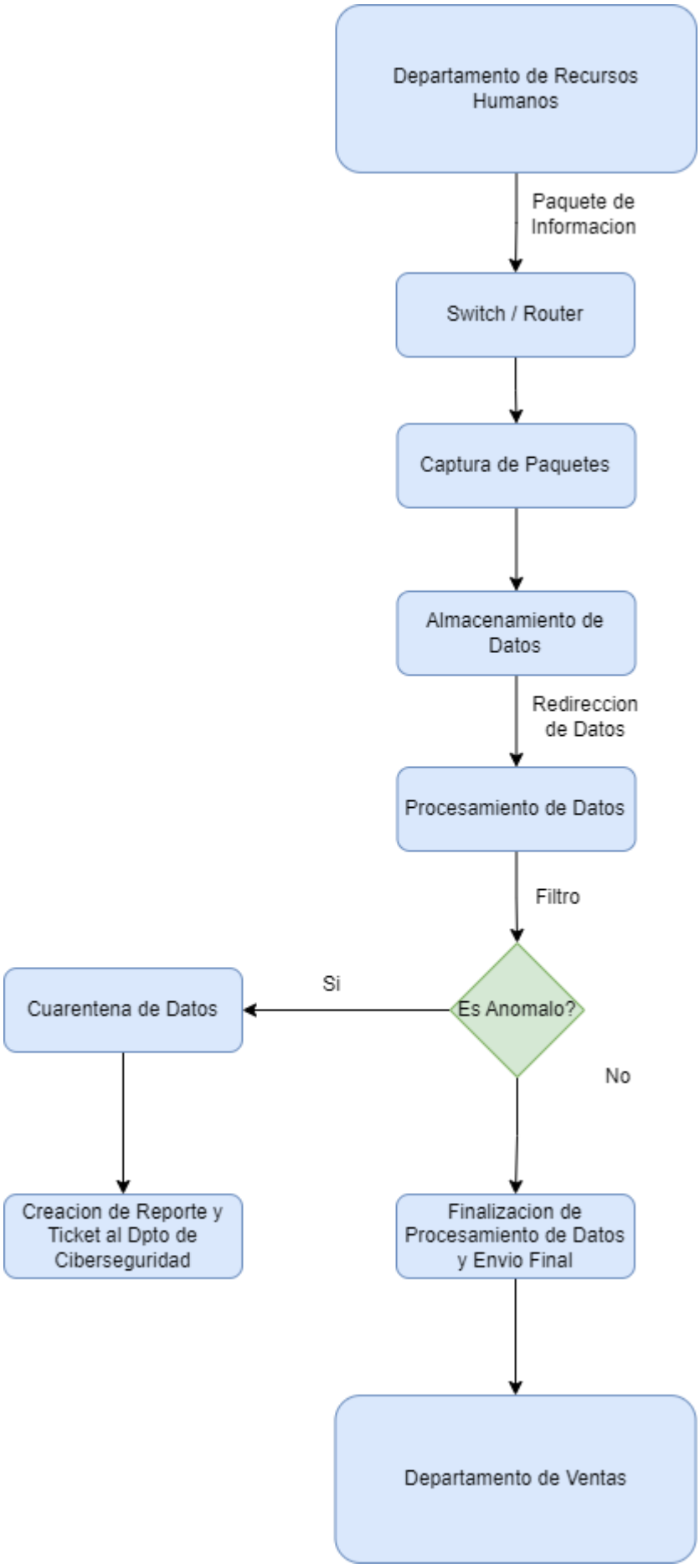
Rendimiento: El análisis de paquetes de red en tiempo real puede ser intensivo en recursos, por lo que se debe utilizar hardware adecuado para manejar grandes volúmenes de tráfico. Además, se pueden implementar técnicas de optimización, como la filtración de paquetes innecesarios o el uso de algoritmos eficientes para el reconocimiento de patrones.

Tiempo de desarrollo: La implementación de un sistema completo de análisis de paquetes de red y reconocimiento de patrones puede llevar tiempo y requerir habilidades especializadas en ciberseguridad y aprendizaje automático.

En resumen, la solución propuesta combina la captura de paquetes de red, el almacenamiento y procesamiento de datos, el análisis de patrones y la implementación de reglas de seguridad para detectar y abordar posibles anomalías de seguridad entre los departamentos de Recursos Humanos y Ventas. Se deben considerar factores de rendimiento y tiempo de desarrollo para asegurar una implementación eficiente y efectiva. Pero una estimación en números crudos puede ser de 6 meses hasta 12 meses.

Medidas en Diagramas




Departamento de Recursos Humanos
Paquete de Informacion
Switch / Router
Captura de Paquetes
Almacenamiento de Datos
Redireccion de Datos
Procesamiento de Datos
Filtro
Es Anomalo?
Si
Cuarentena de Datos
No
Creacion de Reporte y Ticket al Dpto de Ciberseguridad
Finalizacion de Procesamiento de Datos y Envio Final
Departamento de Ventas