5.-Reportes.

Dentro de los reportes necesarios en el SISCOM se encontrarán en 2 rubros, RFL (Reportes Fuera de Línea) y los reportes REL (Reportes En Línea). Lo importante de esta separación es definir aquellos que se conectarán a base de datos críticas o de constante cambio y delicadas, para obtener la información y que tienen un alto grado de concurrencia de inserciones o actualizaciones y aquellas que son más estáticas por decirlo de alguna manera, o que tienen cambios poco significativos y que además su concurrencia es menor en relación a inserciones o actualizaciones.

Seguridad e Integridad de la Información.

Principios de operación.

Garantizar que la seguridad sea lo más efectiva posible es un arduo trabajo. Es un área tan delicada como definir los requisitos funcionales de un sistema, si falta uno o uno queda incompleto nos vemos envueltos en modificaciones que retrasan el despliegue o bien el sistema no cumple con lo requerido en su liberación para ser operado. El principio de "whitelist" (lista blanca) o de permitir lo mínimo indispensable siempre viene bien para la seguridad, siempre y cuando se haga de manera metódica y cuidando los detalles.

Definir lo que solo estará permitido ayuda a evitar dejar huecos de seguridad que nos podría suceder en su contraparte, denegar todo lo que no está permitido. En un ejemplo práctico: una "blacklist" o lista negra nos permite denegar a toda una lista de IP o bien de usuarios, pero si olvidásemos una en particular podríamos dejar una vulnerabilidad que permita un fallo crítico. Por el otro lado, sí solo permitimos aquello que deseamos, por ejemplo, una sola IP o un solo usuario, automáticamente lo demás queda descartado. Si bien no garantiza la seguridad en un 100% nos da un margen de error mínimo, evitando así "olvidar" aquellas cosas que no queremos permitir.

Red Privada Virtual (RPV).

Una solución a lo mínimo permitido son las Redes Privadas, dónde únicamente estarán conectados por medio de un canal seguro los 21 Órganos Desconcentrados Distritales y Municipales. Está solución es por medio de una tecnología de Telmex denominada RPV, donde por medio de un dispositivo (adicional al módem de Infinitum) se conecta el Órgano Desconcentrado directo a un túnel privado con nuestro servidor donde se alojará la aplicación del SISCOM. Dichos canales garantizan su seguridad, ya que no son visibles en internet y son enlaces directos con el destino central. En este caso, el destino central es un servidor en un Data Center Virtual, mismo que está detrás de un Firewall perimetral. Los enlaces al ser directos, no tiene salida a internet, disminuyendo los

riesgos de ataques. Además, el servidor no estará expuesto a Internet, lo que impide un posible ataque de DDoS o de modificación de datos.

Modelado de Amenazas.

El análisis de modelo de amenazas (TMA) es un análisis que ayuda a determinar los riesgos de seguridad que pueden acaecer en un producto, aplicación, red o entorno, así como la forma en la que se aparecen los ataques. El objetivo consiste en determinar cuáles son las amenazas que requieren mitigación y los modos de hacerlo.