202 Destruccuion De Las Copias De Seguridad Almacendas

202 DESTRUCCION DE LAS COPIAS DE SEGURIDAD ALMACENADAS

202.1 Responsabilidad para Aplicar e Implementar la Política:

El Director de Tecnologías de la Información es responsable de crear, actualizar e implementar esta Política.

202.2 Creación y Mantenimiento de Copias de Seguridad:

La División de Tecnologías de la Información garantizará que las Copias de Seguridad de los Registros Electrónicos se mantengan y purguen de acuerdo con esta Política.

Procedimiento:

A) La Copia de Seguridad de los Registros Electrónicos se producirá al final de cada mes (“Copia de seguridad Mensual”).

B) Se puede realizar y mantener una Copia de Seguridad Mensual utilizando un método y soporte de almacenamiento seleccionado por la División de Tecnologías de la Información (inclusive un medio distinto del medio en el que se creó el Registro Electrónico).

C) Una Copia de Seguridad Mensual debe ser almacenada en una ubicación segura externa.

D) Cada Copia de Seguridad Mensual debe conservarse durante al menos

tres (3) años a partir de su creación, con la advertencia de que una Copia de Seguridad Mensual para el mes de diciembre debe conservarse indefinidamente.

202.3 Creación de una Retención de Registros:

Una Retención de Registros es necesaria tras la iniciación o si se anticipa la iniciación de las investigaciones regulatorias o gubernamentales y en los procedimientos administrativos o judiciales con respecto a la Arquidiócesis y/o sus funcionarios, directores, agentes o empleados. En caso de que un empleado se entere de cualquier procedimiento o anticipe la iniciación de un procedimiento, debe informarlo inmediatamente al Director de la División, quien deberá comunicarse de inmediato con el Director de Tecnologías de la Información y el Asesor Jurídico Arquidiocesano para iniciar una Retención de Registros.