

203 Destrucción De Las Copias De Seguridad Almacenas

203 DESTRUCCIÓN DE LAS COPIAS DE SEGURIDAD ALMACENADAS

203.1 Destrucción Periódica:

Excepto cuando un Departamento / División adopta formalmente un período de retención más largo, todas las Copias de Seguridad Mensuales deben ser depuradas de acuerdo con esta Política.

203.2 Garantizar que la Retención por Litigio no se haya Realizado antes de la Destrucción:

El Director de Tecnologías de la Información es responsable de garantizar que una Copia de Seguridad Mensual no esté sujeta a una Retención de Registros antes de la destrucción.

203.3 Programa de Destrucción Trienal:

Una copia de seguridad mensual que se haya conservado durante al menos tres (3) años desde su creación debe purgarse utilizando los procedimientos adecuados de destrucción de datos electrónicos, con la excepción de que no se debe purgar una Copia de Seguridad Mensual para el mes de diciembre.

203.4 Destrucción de Copias de Seguridad Mensuales Existentes:

Las Copias de Seguridad Mensuales existentes a partir de la fecha de entrada en vigencia de esta política que hayan sido creadas con más de tres (3) años de anterioridad deben depurarse utilizando los procedimientos adecuados de destrucción de datos electrónicos, con la advertencia de que una copia de seguridad mensual para el mes de diciembre no debe ser purgada.

203.5 Registros Retenidos:

En ausencia de una Retención de Registros, la implementación ordinaria de esta Política debería resultar en la conservación de las siguientes Copias de

Seguridad Mensuales:

- 1) las de menos de tres años y
- 2) Copias de Seguridad mensuales del mes de diciembre (independientemente de la edad).