



Universidad de Puerto Rico
Administración Central
Oficina de Sistemas de Información

Normas y Procedimientos para la Disposición de Dispositivos de Almacenamiento de Datos

Oficina de Sistemas de Información
Revisión septiembre 2022

NORMAS Y PROCEDIMIENTOS PARA LA DISPOSICIÓN DE DISPOSITIVOS DE ALMACENAMIENTO DE DATOS

INTRODUCCIÓN Y MOTIVO

Los datos y programas instalados en computadoras, dispositivos electrónicos y medios de almacenaje representan un riesgo de seguridad y confidencialidad al momento de disponer o transferir dicho equipo. Este riesgo se debe atender mediante procesos de limpieza y disposición segura que garanticen que la información contenida en esos dispositivos no se vea comprometidos y accesibles a terceros.

La clave para decidir cómo administrar los medios y la disposición de éstos es considerar primero la información, luego el tipo de medio. La categorización de seguridad y confidencialidad de la información tienen que estar basado en la *Política Institucional para la Clasificación de Datos de la Universidad de Puerto Rico*, para tomarse como marco de referencia sobre cómo tratar y disponer con los medios que contienen esta información.

Estas normas y procedimientos están basadas en el NIST SP 800-88.

NORMAS GENERALES

Previo a la transferencia o disposición de equipo, es imprescindible que se disponga de forma segura los datos y programas. Se deben eliminar cualquier acceso potencial a datos privados cuando la transferencia del equipo sea hacia un destino desconocido o hacia una persona u oficina que no está autorizada para acceder dicha información privada. El departamento o individuo directamente responsable por los datos privados en la computadora o dispositivo electrónico deberá asegurarse que los datos han sido removidos de forma segura, previo a disponer del equipo y antes de que esté fuera de su control. El personal técnico de las Oficinas de Sistemas de Información de las unidades podrá asistir en dicho proceso y certificar que en efecto la información ha sido eliminada de forma segura.

Por otra parte, cuando se decomisa un equipo con dispositivos de almacenamiento, se debe proceder con la remoción de éstos y asegurar que la información que pudo haber estado almacenada no es accesible. Esto puede hacerse utilizando procesos de escritura en estos dispositivos de almacenamiento con programas especializados, o mediante la destrucción física, como se indica más adelante. Las Oficinas de Propiedad coordinarán con la Oficina de Sistema de Información de la unidad correspondiente para la remoción y disposición de estos dispositivos, asegurando que no salen del control de la institución hasta tanto no se haya completado este proceso.

Existen compañías que se dedican a la eliminación de datos y destrucción de equipos de almacenaje que pueden ser utilizadas para estos procesos. Sin embargo, es importante que estas compañías estén certificadas para esto y que emitan certificado con los detalles de la destrucción.

LIMPIEZA DE DATOS EN MEDIOS DE ALMACENAMIENTO

Existen diferentes tipos de limpieza y borrado para cada tipo de medios de almacenamiento. Se han dividido los procedimientos limpieza de datos en cuatro categorías: **borrado, eliminación y destrucción**.

Existe decomisado en donde los medios simplemente se desechan sin que se les dé una disposición especial. Se puede disponer de algunos medios sin ningún tipo de limpieza si la divulgación de la información no tiene impacto en la organización, sus activos, personal o estudiantes.

Bajo cualquier otra circunstancia, los usuarios tienen que categorizar la información y evaluar el medio en el que se graba, además del riesgo basado en la *Política Institucional de Clasificación de Datos*. Basado en esto, se debe decidir el tipo de limpieza que debe ocurrir de los medios de almacenaje.

Tipo de Limpieza	Descripción
Sobreescritura	La simple eliminación de archivos no es suficiente para una limpieza efectiva. La limpieza no debe permitir que la información sea recuperada por utilidades de recuperación de datos y archivos. <u>Para esto, sobrescribir es un método aceptable para borrado de los medios.</u> Hay productos de software o hardware de sobreescritura. El objetivo de seguridad del proceso de sobreescritura es reemplazar los datos escritos con datos aleatorios. Sin embargo, la sobreescritura no se puede usar para medios dañados o que no se pueden escribir por daños físicos. El tipo y el tamaño del medio también pueden influir en decidir si la sobreescritura es una limpieza adecuada.
Eliminación	La eliminación de información es un proceso de limpieza de medios que protege la confidencialidad de información contra un proceso de recuperación con equipo especializado de laboratorio. <u>La ejecución de borrado seguro del <i>firmware</i> de los dispositivos y el desmagnetizar (<i>degaussing</i>) son ejemplos de métodos aceptables para la eliminación.</u> La desmagnetización consiste en exponer los medios magnéticos a un fuerte campo magnético. La desmagnetización puede ser un método eficaz método para limpiar información de medios dañados, o medios con

	almacenamiento excepcionalmente grande. La desmagnetización no es efectiva para limpiar medios no magnéticos, como los discos tipo <i>solid state</i> (SSD).
Destrucción	La destrucción de los medios es la mejor forma de limpieza. La destrucción física se puede lograr usando u variedad de métodos, incluyendo desintegración, incineración, pulverización, trituración y derritiendo. La destrucción de los medios debe ser realizada únicamente por personal capacitado y autorizado dado los aspectos de seguridad, uso de materiales peligrosos y la disposición adecuada de los residuos. Por esta razón, <u>usualmente son utilizadas compañías externas para la destrucción.</u>