1. OBJETIVO

Definir las directrices generales para el borrado seguro de la información en la Institución de Educación Superior CINOC, a través de la descripción de las actividades de solicitud, preparación, ejecución e informe del resultado del borrado seguro, con el fin de preservar la confidencialidad de la información.

2. ALCANCE

El presente procedimiento aplica para la mesa de servicios tecnológicos, funcionarios y contratistas que almacenan información en copias de seguridad y que son administradas desde el Departamento de Tics.

3. DEFINICIONES

ACTIVO DE INFORMACIÓN: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.

BORRADO SEGURO: Se refiere al procedimiento necesario para garantizar que la información existente en un medio de almacenamiento, no pueda ser recuperada a través de alguna técnica especializada.

DISPOSITIVO DE ALMACENAMIENTO: Se refiere a cualquier elemento que se utiliza para almacenar información tales como, discos duros, memorias USB, entre otros.

INFORMACIÓN DIGITAL: Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos, en forma de archivos digitales o de intercambio.

LISTA DE ARCHIVOS: Es un término genérico que referencia al conjunto de elementos que cada sistema de archivos utiliza para guardar, tanto la información que identifica los archivos (nombre, tipo, fecha de creación, etc.), como un índice que recoge la ubicación física del contenido del archivo.

DESMAGNETIZACIÓN: La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

DESTRUCCIÓN FÍSICA: Es la inutilización del soporte que almacena la información para evitar la recuperación posterior de los datos que almacena

4. CONDICIONES GENERALES

El ciclo de vida de la información, de forma simplificada, consta de tres fases: generación, transformación y destrucción. Toda información tiene una vida útil tanto si está en formato digital (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria, etc.) como en formatos tradicionales (papel, carpetas, entre otros). Cuando la vida de la información llega a su fin, se deben emplear mecanismos de destrucción y borrado seguro para evitar que esta quede al alcance de terceros.

Con el borrado seguro y destrucción de soportes de información no solo se busca proteger la difusión de información confidencial de la entidad, sino también proteger la fuga de datos personales de los usuarios de los servicios que puedan contener los soportes.

Son comunes los incidentes de seguridad de la información, presentados en las organizaciones por la falta de diligencia en el borrado de la información que, por ejemplo, son arrojados en lugares públicos (papeleras, contenedores, etc.) o no son debidamente destruidos (triturados, desmagnetizados, sobrescritos, etc.), encontrando información evidentemente llamativa como datos bancarios, médicos, de menores, etc.

5. DESARROLLO

Nro.	Actividad	Responsable	Registro
1	Recibir la solicitud: El responsable del activo de información que contenga la información a borrar debe realizar la solicitud por los canales formales de la mesa de servicio por medio de Ticket o correo electrónico al Departamento de Tics.	Responsable del Activo de Información	Formato de solicitud
2	Verificación de la Solicitud y estado del activo: Una vez recibida la solicitud de destrucción de información el encargado de T.I debe identificar la información, su estado y clasificarla de acuerdo al inventario de activos de información y causas tales como: - Retiro - Traslado - Daño - Cambio de equipo - Vida útil de la información gestionada.	Líder del Departamento de Tics	Formato de registro de identificación del estado y clasificación de acuerdo al inventario de activos de información.
3	Registro de información para el borrado: El líder de departamento de Tics encargado de realizar la actividad de borrado seguro para el medio de almacenamiento digital como; Discos duros, CD, DVD,S bases de datos de clientes y/o usuarios, copias de seguridad.	Líder del Departamento de Tics	Registro de información para el borrado.
4	Intento de recuperación de información: Una vez borrada la información se debe ejecutar un intento de recuperación de datos esto con el fin de garantizar el que la eliminación se realizó.	Líder del Departamento de Tics	
5	Certificado digital del borrado: Una vez se realice la eliminación de la información el líder de tecnología debe certificar el borrado seguro y proceder a custodiarlo y entregarlo al usuario que realizo la solicitud.	Líder del Departamento de Tics	Registro de Certificación digital del borrado.
6	Generación de acta: Al finalizar de ciclo del borrado seguro las partes involucradas en el procedimiento deben generar un acta donde se identifiquen responsables, nombre del activo de	Líder de Sistemas / Dueño del activo	Formato acta de eliminación.

	información, clasificación, fecha de borrado, tamaño, fuente de información del borrado, estado, certificado digital, firmas de responsables y subir la evidencia al Ticket de la mesa de servicio y cerrarlo.		

6. FORMATOS Y REGISTROS DEL SISTEMA

- Formato de solicitud de eliminación
- Formato de registro de identificación del estado y clasificación de acuerdo al inventario de activos de información.
- Registro de información para el borrado.
- Registro de Certificación digital del borrado.
- Formato acta de eliminación.

7. DOCUMENTOS EXTERNOS

Política de Gestión de la Información de la IES.

NTC ISO 1799:2005 “Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.”

ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información (SGSI)”

ISO/IEC 27002:2013 Código de buenas prácticas de la gestión de la seguridad de la información.

8. PUNTOS DE CONTROL

ACTIVIDAD	RESPONSABLE	OBJETIVO DEL CONTROL
Identifica que la información registrada en el formato de eliminación de documentos digitales haya sido realizada con los parámetros de seguridad establecidos.	Coordinador de Tics	Constatar que el equipo de computo y todos los medios digitales de almacenamiento no cuenten con la información registrada en el formato de eliminación de documentos electrónicos.

9. HISTORIAL DE CAMBIOS

FECHA	VERSION	CAMBIOS
22/08/2023	1	Versión inicial del documento