PROCEDIMIENTO	Código: **S03.04.11.01**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE ELIMINACIÓN DE INFORMACIÓN EN LOS SISTEMAS INTERNOS

	Nombres y Apellidos	Cargo	Firma y Sello
Elaborado por:	Manuel Aguilar Cori	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por: AGUILAR CORI Manuel Isidro FAU 20380799643 hard Fecha: 23/09/2025 14:44:17
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:34:02
Revisado por:	Apolinar Madrid Escobar	Jefe (dt) de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por: MADRID ESCOBAR Apolinar Junior FAU 20380799643 hard Fecha: 23/09/2025 16:37:53
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios (indicar sección de corresponder)	Fecha
01	Versión inicial	24/09/2025

1. BASE LEGAL

1.1. ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos” (en adelante ISO/IEC 27001).

1.2. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos (en adelante NTP-ISO/IEC 27001).

1.3. ISO/IEC 27002 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante ISO/IEC 27002).

1.4. NTP-ISO/IEC 27002:2022 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante NTP-ISO/IEC 27002).

1.5. Versión Actualizada de la Directiva N° 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.

1.6. Reglamento Interno de los Servidores Civiles - RIS de la Agencia de Promoción de la Inversión Privada – PROINVERSIÓN.

1.7. Código de Ética de la Agencia de la Promoción de la Inversión Privada PROINVERSIÓN.

2. DEFINICIONES Y SIGLAS

2.1. Definiciones

2.1.1. **Activo de Información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

2.1.2. **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

2.1.3. **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

2.1.4. **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

2.1.5. **Eliminación segura:** Proceso que garantiza la eliminación permanente e irrecuperable de datos de un dispositivo de almacenamiento

2.1.6. **Evento o Suceso:** Ocurrencia o cambio de un conjunto particular de circunstancias.

Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.
Nota 2: Un evento puede consistir en algo que no sucede.
Nota 3: Un evento a veces puede ser referido como un "incidente " o "accidente”.

2.1.7. **Evento de Seguridad de Información**: Ocurrencia identificada de un sistema, servicio o el estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación antes desconocida que puede ser la seguridad relevante.

2.1.8. **Gestión de Incidentes de Seguridad de Información:** Aseguramiento que el acceso lógico a los activos de información está autorizado y Procesos para detectar, informar, evaluar, responder frente a, y aprender de incidentes de seguridad de la información.

2.1.9. **Incidente de Seguridad**: Es un evento adverso que puede generar un impacto en un sistema de información o en una red de servicios informáticos comprometiendo la confidencialidad, integridad y disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o acciones de amenaza que puedan poner en riesgo los mecanismos de seguridad existentes.

2.1.10. **Incidente de Seguridad de Información**: Evento único o una serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

2.1.11. **Integridad:** Propiedad de exactitud y lo completo.

2.1.12. **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

2.1.13. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

2.2. Siglas:

- CGTD: Comité de Gobierno y Transformación Digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- OSCD: Oficial de Seguridad y Confianza Digital.
- ETRIS: Equipo Técnico de Respuestas ante Incidentes de Seguridad.

3. RESPONSABILIDADES

3.1. Del Oficial de Seguridad y Confianza Digital (OSCD)

3.1.1. Verificar y certificar el cumplimiento de eliminación de información.
3.1.2. Gestionar la custodia de evidencias de eliminación de información
3.1.3. Proponer alternativas de métodos para eliminación segura de información.
3.1.4. Realizar coordinaciones con el Equipo de tecnologías de información para la realización de actividades relacionadas a la eliminación segura de información.
3.1.5. Implementar y mantener controles de seguridad de la información que puedan reforzar de manera efectiva el presente procedimiento.
3.1.6. Planificar y realizar la revisión de cumplimiento de controles.

3.2. Del Especialista de Tecnologías de Información y Redes

3.2.1. Ejecutar el método de eliminación segura.
3.2.2. Proponer alternativas técnicas de eliminación segura de información a adherir en la gestión del área de tecnologías de información.
3.2.3. Coordinar con proveedores de servicio del tipo custodio de información física y digital, la eliminación segura de información
3.2.4. Identificar y seleccionar método de eliminación.

4. GENERALIDADES

4.1. Activos de información considerado para eliminación segura:

4.1.1. Discos duros, SSD, USBs, cintas magnéticas, dispositivos móviles, equipos en desuso, etc.
4.1.2. Datos en soportes físicos o digitales (incluyendo backups y medios de almacenamiento en la nube).

4.2. Métodos de eliminación segura considerados:

	Método	Descripción	Aplicación
1	**Borrado seguro (Software)**	Sobreescritura con patrones (ej. 3 pasos DoD 5220.22-M, 7 pasos Gutmann).	HDD, SSDs (con verificación posterior)
2	**Destrucción física**	Trituración, incineración, desmagnetización (degaussing) o pulverización	Medios obsoletos o dañados
3	**Cifrado + Borrado**	Eliminación de claves de cifrado (si los datos estaban encriptados)	SSDs, almacenamiento en la nube
4	**Eliminación certificada**	Uso de servicios especializados con certificación **ISO 27001** o **e-Stewards**	Medios críticos u outsourcing

En el caso que se requiera una destrucción física de la información y que sea realizada por personal tercero, se deberá asegurar que los terceros se encuentren autorizados para el fin y que expidan certificados de destrucción, en cuyo acto cuente con participación de personal técnico de PROINVERSION en calidad de veedores

4.3. Excepciones

4.3.1. Medios reutilizados internamente: Requieren formato seguro más auditoría.

4.3.2. Fallos en el método: Escalarlo para destrucción física inmediata.

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Programar eliminación de información			
1	Identificar la información a eliminar - clasificación y soporte (si está en medios electrónicos (discos, USB, cloud) o físicos (papel, cintas)	Área de TI	OSCD
2	Verificar que la solicitud de eliminación haya sido aprobada por el propietario de la información ¿Está aprobado? Si: Ir a tarea 3 No: Ir a tarea 1	Área de TI	OSCD
3	Elaborar registro de programación de eliminación de información	Área de TI	OSCD
Organizar eliminación de información			
4	Coordinar eliminación de información	Área de TI	OSCD
Ejecutar eliminación de información			
5	Identificar el soporte de información a eliminar ¿Es soporte electrónico? Si: Ir a tarea 6 No: Ir a tarea 7	Área de TI	Especialista de Tecnologías de Información y Redes
6	Seleccionar método de eliminación de información electrónica y responsable Considerar como referencia en Anexo N° 1 Tabla N° 1 “Herramientas recomendadas”	Área de TI	Especialista de Tecnología de Información y Redes
7	Seleccionar método de eliminación de información en soporte físico Considerar como referencia en Anexo N° 1 Tabla N° 1 “Herramientas recomendadas”	Área de TI	Especialista de Tecnología de Información y Redes
8	Ejecutar eliminación de información	Área de TI	Especialista de Tecnología de Información y Redes
Certificar eliminación de información			

9	Verificar que la información fue eliminada siguiendo el método seleccionado	Área de TI	OSCD
10	Confirmar eliminación de información con certificado o informe de eliminación (Interno o tercero)	Área de TI	OSCD
Documentar eliminación de información			
11	Conservar los registros de eliminación de información (informes), los cuales se almacenarán en SharePoint, en una carpeta asignada exclusivamente para el acopio de los documentos de sustento	Área de TI	OSCD
12	Enviar comunicación de eliminación de información	Área de TI	OSCD
Fin			

6. ANEXOS

6.1. Herramientas recomendadas
6.2. Flujograma de procedimiento

Anexo N° 01

Tabla N° 1 "Herramientas recomendadas"

	Tipo	Herramientas
1	Software	DBAN, Blancco, CCleaner (modo seguro)
2	Hardware	Trituradoras de discos (ej. SEM Shredder)
3	Físico	Trituradora de papel
4	Servicios	Proveedores con certificación ISO 27001:2022, e-Stewards o R2

Anexo N° 02

Flujograma de procedimientos