En Entorno y Compañía, entendemos que la información es uno de nuestros activos más valiosos y la información requerida a nuestros clientes necesita de un direccionamiento para su custodia, manejo responsable y devolución o destrucción cuando finalice la relación comercial. La dirección se compromete firmemente a proteger la confidencialidad, integridad y disponibilidad de toda la información. Asumimos la responsabilidad de implementar, mantener y mejorar continuamente lo que respecta a la Seguridad de la Información, asegurando el cumplimiento de todos los requisitos legales y reglamentarios pertinentes.

Establecemos los lineamientos y procedimientos técnicos para la eliminación segura de la información y la destrucción de toda la documentación física y digital, garantizando que los datos relacionada la empresa, datos personales o documentos confidenciales, personales y de salud según las normas vigentes, no puedan ser recuperados o reconstruidos por terceros no autorizados.

MARCO LEGAL Y NORMATIVA

Esta política está amparada por las siguientes leyes:

- Ley 1581 de 2012: Protección de Datos Personales (Habeas Data).
- Ley 23 de 1981 y Resolución 1995 de 1999: Gestión de Historias Clínicas (respetando los tiempos de retención legal).
- Decreto 1008 del 14 de junio de 2018 Política de Gobierno Digital
- Ley 2015 de 31 de enero 2020. Por medio del cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones.
- ISO/IEC 27001:2022: Control 8.10 (Eliminación de información).
- Decreto 1074 de 2015: Capítulo 25 sobre tratamiento de datos personales.
- Resolución 1843 de 2025. Política custodia de la Historia Clínica

ALCANCE

Aplica a todos los activos de información de la Sociedad Entorno & Compañía LTDA (servidores, estaciones de trabajo, discos duros, memorias USB, teléfonos móviles) que contengan datos sensibles, historias clínicas o información administrativa.

RESPONSABILIDADES

Direccionamiento estratégico (Gerencia), responsable de la Calidad y Tecnología de la información (IT): Asegurarse de la correcta implementación, seguimiento y cumplimiento de esta política.

Colaboradores de la Sociedad Entorno & Compañía Ltda: Cumplir con los procedimientos establecidos para la eliminación segura de la información.

Proveedores externos de servicios de destrucción: Seguir los protocolos establecidos (según las normas ISO 27001 y las establecidas y aplicables en Colombia para tales efectos); y proporcionar las evidencias de destrucción en los casos aplicables con el respectivo certificado.

CLASIFICACIÓN Y MÉTODOS DE ELIMINACIÓN

Según el tipo de información manejada en Entorno & Compañía Ltda, podemos identificar los siguientes tipos de soporte:

TIPO DE SOPORTE	MÉTODO DE ELIMINACIÓN	HERRAMIENTA/TÉCNICA
Medios electrónicos reutilizables.	Sobre escritura segura.	Eraser (DoD 5220.22-M)
Medios electrónicos dañados.	Destrucción física	Desmagnetización o trituración.
Documentos en papel.	Destrucción física	Trituración de documentación.

DISPOSICIONES GENERALES

Todo evento de destrucción o eliminación debe ser socializado con las partes involucradas. La persona responsable de borrar los datos o destruir el soporte debe informar al propietario del activo en cuestión, acerca del borrado o eliminación de datos, y posterior al evento debe ser actualizado el inventario de activos.

Todo evento de destrucción o eliminación debe estar respaldado con su respectiva acta (FOR.DIE.003), la cual debe contener:

- Fecha y hora de la destrucción.
- Tipo de soporte destruido.
- Responsable de la supervisión del proceso.
- Firma de la persona o proveedor encargado de la destrucción

- Historias Clínicas: Nunca se debe eliminar una historia clínica sin previa validación del Comité de Historias Clínicas y la verificación de que el tiempo de retención (establecido por la Ley 2015 de 2020, Resolución 1843 de 2025. Política custodia de la Historia Clínica y normatividad vigente) se haya cumplido.

Dispositivos Móviles: En caso de tablets o celulares usados en consulta, se debe realizar un "Factory Reset" tras el cifrado previo de los datos, o utilizar herramientas de borrado certificadas para móviles.

Terceros: Si la destrucción la realiza un tercero, se debe exigir un Certificado de Destrucción Final que exonere de responsabilidad a la Sociedad Entorno & Compañía Ltda, ante la Superintendencia de Industria y Comercio (SIC).

PROCEDIMIENTOS DE ELIMINACIÓN Y DESTRUCCIÓN DE DATOS.

Destrucción de información física (papel).

Todos los documentos físicos relacionados con colaboradores, proveedores, y clientes que ya no son necesarios, deben ser destruidos mediante un proceso de triturado. Por ejemplo: hojas de vida, contratos vencidos, información de pagos, facturas obsoletas, entre otros.

Destrucción de información física (medios magnéticos)

Todo hardware de almacenamiento físico que, por efectos de cumplimiento de vida útil como discos duros, memorias USB, CD/DVD, que contengan o hayan contenido información sensible, deben ser destruidos (triturados).

Restablecimiento de equipos de computación y teléfonos (HARD RESET).

Todo equipo de cómputo o comunicaciones (celulares/teléfonos inteligentes) cuyo estado en el inventario sea cambiado y aun se encuentre en condiciones de uso teniendo en cuenta su vida útil, debe ser restaurado a modo de fabrica con un borrado de eliminación de datos seguro.

Destrucción de información digital

En cuanto a la información digital, la Sociedad Entorno & Compañía Ltda, ha definido el uso de la herramienta Eraser (software de código abierto para Windows) para la eliminación lógica definitiva de archivos en discos mecánicos y medios extraíbles.

Paso a Paso Con Eraser:

Fase 1: Preparación:

Solicitud y aprobación: El área de IT debe verificar la solicitud y aprobación por parte de la Gerencia para proceder a la destrucción o eliminación.

Identificación: El área de IT o el responsable de la destrucción o eliminación debe identificar los archivos o volúmenes que han cumplido su tiempo de retención legal.

Copia de Seguridad: Antes de eliminar, confirmar que no se requiere una copia de respaldo para fines legales o de auditoría.

Fase 2: Configuración de Eraser:

Para cumplir con estándares internacionales, se debe configurar el método de borrado:

Abrir Eraser -> Settings. En "Default file erasure method", seleccionar US DoD 5220.22-M (8-306. /E, C and E) (7 pasadas) para información de extrema sensibilidad.

Fase 3: Ejecución del Borrado:

Selección: Haga clic derecho sobre el archivo, carpeta o unidad de disco que desea eliminar. (Si se está utilizando Windows 11, seleccionar Mostrar Más Opciones).

Ejecución: Seleccione el menú "Eraser" y luego "Erase".

Confirmación: El sistema solicitará una confirmación final. Una vez aceptada, el proceso comenzará a sobreescribir los sectores del disco con datos aleatorios.

Fase 4: Verificación y Registro

Verificación: Intentar recuperar una muestra de datos con herramientas de recuperación básica para asegurar que el proceso fue exitoso.

Acta de Destrucción: Se debe generar un registro que contenga: Fecha y hora del proceso. Descripción del activo eliminado. Método utilizado (Ej: Eraser - DoD 5220.22-M). Responsable que ejecutó la acción.

Se debe llevar una bitácora general de todos los procesos de eliminación y destrucción de datos:

Fecha	Tipo de soporte	Ubicación de archivo	Responsable del elemento a eliminar o destruir	Autorización para eliminación o destrucción	Tiempo de retención.

MANEJO DE INCIDENTES CON DATOS RECOPILADOS.

En el evento de identificar un manejo incorrecto con la información recopilada para la debida prestación del servicio, por parte de un colaborador o tercero, procederemos con el siguiente paso a paso de Preparación, Detección y Análisis, Contención, Erradicación, Recuperación y Revisión . Documentando lo sucedido como Lecciones Aprendidas y evitar su repetición

1. **Preparación:** Desarrollar el Plan de Respuesta a Incidentes (IRP) y definiendo los roles y responsabilidades, a cargo del responsable del área donde ocurra y Recursos Humanos de Entorno & Compañía Ltda. Previa Identificar y clasificación de datos críticos y vulnerabilidades.

   La comunicación del incidente se realizará a través del IPLO formato FOR.GAD.097 que recopila la Dirección Administrativa y abre el incidente para su correspondiente manejo.

   Correo: administración@entornoycia.co

2. **Detección y Análisis:** Se sensibiliza sobre la importancia de monitorear alertas y actividad sospechosa. Recopilar evidencias (registros, documentos físicos o digitales) y analizar para entender el alcance, severidad e impacto.

   Determinar la causa raíz (ej. phishing, credenciales comprometidas) para definir el plan de respuesta al incidente.

3. **Contención:** Aislar sistemas afectados para detener la propagación del daño (ej. desconectar de la red). Bloquear tráfico malicioso y prevenir mayor acceso.

4. Erradicación: Eliminar la amenaza (malware, atacantes) y restaurar la integridad de los sistemas comprometidos.

5. Recuperación: Restaurar operaciones a la normalidad, verificando la funcionalidad. Monitorear sistemas para detectar actividad residual.

6. Revisión (Lecciones Aprendidas): Analizar el incidente y el proceso de respuesta. Identificar áreas de mejora y actualizar el IRP.

Fin del documento.

Leyla Verónica Rossi S.

Gerente