POLÍTICA DESTRUCCIÓN SEGURA DE INFORMACIÓN

EML S.A.S
Bogotá, Colombia

1. Objetivo:

Establecer los lineamientos y procedimientos para la destrucción segura de documentos físicos y digitales en EML S.A.S., garantizando la protección de la información confidencial de colaboradores, proveedores, clientes, y cualquier otro tercero, en cumplimiento con la Norma ISO 27001 y las mejores prácticas de seguridad de la información.

2. Alcance

Esta política aplica a todos los documentos físicos y digitales que contengan información confidencial, personal, o sensible relacionada con colaboradores, proveedores, clientes, y otros terceros vinculados con la operación de EML S.A.S.

3. Lineamientos

La destrucción de información sensible será gestionada anualmente o ante algún evento significativo con el propósito de mantener y mejorar el SGSI de EML S.A.S.

4. Responsabilidades

- **Comité de Seguridad de la Información:** Asegurarse de la correcta implementación, seguimiento y cumplimiento de esta política.
- **Colaboradores de EML S.A.S.:** Cumplir con los procedimientos establecidos para la eliminación segura de información.
- **Proveedores externos de servicios de destrucción**: Seguir los protocolos acordados y proporcionar las evidencias de destrucción en los casos aplicables.

5. Procedimientos de Destrucción de Información

5.1. Documentación Física

- **Proceso de Destrucción:**
  - ❖ Todos los documentos físicos relacionados con colaboradores, proveedores, y clientes que ya no son necesarios según las políticas de retención de datos, deben ser destruidos mediante un proceso de triturado certificado.
  - ❖ Ejemplos de documentos a destruir incluyen hojas de vida, contratos vencidos, información de pagos, facturas obsoletas, entre otros.
- **Evidencia de Destrucción:**
  - ❖ La destrucción de documentos físicos debe estar documentada mediante un acta que incluya:
    - Fecha de la destrucción
    - Tipo de documento destruido
    - Responsable de la supervisión del proceso
    - Firma de la persona o proveedor encargado de la destrucción
- **Retención de Actas:**
  - ❖ Las actas de destrucción deben almacenarse durante un periodo de 5 años y estar disponibles para auditorías.

5.2. Documentación Digital

- **Proceso de Eliminación:**
    - ❖ Los archivos digitales que contengan información confidencial o sensible deben ser eliminados utilizando herramientas de borrado seguro, que aseguren la imposibilidad de recuperación de los datos. Esto incluye:
        - Hojas de vida digitales de colaboradores, una vez finalizado el proceso de selección, deben ser eliminadas completamente de las bases de datos y sistemas de almacenamiento.
        - Información confidencial de proveedores y clientes obsoleta debe ser destruida de manera irreversible mediante técnicas como el borrado criptográfico o sobreescritura de datos.
- **Evidencia de Eliminación:**
    - ❖ Se debe generar una bitácora o registro digital con los siguientes detalles:
        - Fecha de eliminación
        - Tipo de archivo eliminado
        - Método de eliminación utilizado
        - Responsable de la eliminación
- **Retención y Eliminación de Hojas de Vida de Colaboradores**
    - ❖ Las hojas de vida de los candidatos no seleccionados deben ser eliminadas en un plazo máximo de 30 días hábiles tras la recepción.
    - ❖ Las hojas de vida físicas correspondientes a procesos de selección de años anteriores serán destruidas a través de un proceso de triturado certificado, siguiendo el procedimiento descrito en el apartado de Documentación Física.
- **Destrucción de Información de Proveedores y Clientes**
    - ❖ La información confidencial o sensible relacionada con proveedores y clientes, tales como contratos, acuerdos, o facturación, será destruida una vez haya expirado su periodo de retención, conforme a los requisitos legales y contractuales vigentes.

- ❖ Se mantendrán registros de todas las actividades de destrucción de estos documentos, siguiendo los procedimientos de evidencia mencionados.

- **Verificación y Auditoría**
  - ❖ El Comité de Seguridad de la Información realizará revisiones periódicas para verificar el cumplimiento de esta política, incluyendo auditorías de los procesos de destrucción y la revisión de actas o bitácoras de destrucción.
  - ❖ Cualquier incumplimiento o incidente será reportado y tratado según el Protocolo de Gestión de Incidentes de EML S.A.S.

6. Anexo: Requisitos de la Norma ISO 27001

Esta política se establece conforme a los controles de la Norma ISO 27001, en especial los relacionados con el tratamiento seguro de la información y la protección contra accesos no autorizados, así como la disposición segura de los datos, tal como lo establece el control A.8.3.2 (Eliminación de Medios) de la norma.