1. Objetivo

La política de Gestión de la información tiene como objetivo definir las pautas generales para la elaboración, almacenamiento, conservación, seguridad, acceso, publicación y consulta de los activos de información que son recibidos, gestionados o producidos en las diversas áreas de la compañía.

2. Alcance

La gestión de la información comprende la administración de Datos, Documentos y Contenidos Digitales. Ver diagrama Anexo 1.

Las disposiciones contenidas en la presente política aplican para todas las personas que trabajan para AES Chivor, directa o indirectamente; esto incluye a empleados temporales, aprendices, practicantes, consultores, contratistas y proveedores.

3. Principios que rigen la Gestión de la Información

3.1. Confidencialidad: La información (física o electrónica) debe ser revelada únicamente a las personas y entidades autorizadas. Los colaboradores, contratistas y personal autorizado deberán mantener la confidencialidad de la misma.

3.2. Integridad: La información gestionada por cada una de las funciones o procesos de la compañía deberá garantizar que se respalde y transmita de una manera exacta y completa

3.3. Disponibilidad: La empresa brindará los recursos necesarios para garantizar la accesibilidad y disponibilidad de la información en el momento oportuno.

3.4. Seguridad: Este principio corresponde a la necesidad de Identificar y gestionar los riesgos relacionados con la seguridad de la información dentro de los procesos para protegerla de la divulgación no autorizada, modificación indebida o destrucción de los soportes.

4. Requerimientos Legales.

Esta política está en consonancia con el cumplimiento de la siguiente normatividad:

4.1. Ley de Sarbanes-Oxley;(Pub. L. 107-204, 116 Stat.745, también conocida como Public Company Accounting Reform and Investor Protection Act of 2002, y comúnmente llamada SOX o Sarbox, Julio 30 de 202.
4.2. Decreto 2609 de 2012. Ciclo documental propuesto por el Archivo General de la Nación (AGN)
4.3. Ley 1581 de 2012 y Decreto 1377 de 2013. Protección de Datos

4.4. Ley 1712 de 2014. Derecho de acceso a la información Pública o Ley de transparencia

5. Documentos de referencia

- Política de Manejo de la Información (IT)
- Política de Tratamiento y protección de datos personales.
- COM-POL-001 Política de Comunicaciones

6. Definiciones.

6.1. Datos: Incluye toda la información transaccional, analítica e histórica tal como información contable, scada, etc.
6.2. Documentos: Hace referencia a los documentos de archivo. Los documentos pueden ser físicos, electrónicos, digitalizados o una combinación entre cualquiera de éstas.
6.3. Contenidos digitales: Incluye la información que se pública en las páginas web: Extra e intranet; así como en redes sociales.
6.4. Archivo: Conjunto de documentos (físicos, electrónico, mixtos), sea cual fuere su fecha, acumulados en el desarrollo de un proceso por un funcionario en el transcurso de su gestión.
6.5. Archivo de gestión: Es el archivo de la oficina productora, que reune su información en trámite, sometida a continua utilización y consulta administrativa.
6.6. Archivo Central: Unidad administrativa receptora de los archivos de gestión transferidos una vez finalice su tramite y requieran su conservación por requerimiento normativo interno o por legislación local.
6.7. Tablas de Retención documental (TRD): Es el listado de series y subseries documentales con sus correspondientes tipos, producidos o recibidos por las áreas de la compañía; donde adicionalmente se establecen aspectos como:

Clasificación, tiempo de conservación, forma de eliminación, entre otros. Las TRD aplican tanto para información física como para información electrónica.

6.8. Propietarios de la Información: Son todas aquellos líderes de procesos: Gerentes, Directores, Jefes o representantes de estos en cuyas áreas se crea o recibe información a partir de la realización de sus gestiones diarias.

7. Roles y Responsabilidades.

Todas las personas que trabajan para AES Chivor, directa o indirectamente son responsables del cumplimiento de esta política y deben realizar las acciones correspondientes para garantizar su cumplimiento a lo largo del ciclo de gestión de la información.

7.1. Propietarios de la Información

Responsables de:

- Determinar quiénes, cómo, dónde (Archivo de Gestión o Archivo Central) y durante cuánto tiempo se debe conservar la información, gestionando su inmediata clasificación. Lo anterior acorde con los lineamientos definidos en la presente política y los documentos de referencia listados en el numeral 5.

- Cumplir estrictamente los lineamientos emanados de la presente política y todas aquellas relacionadas con la gestión y seguridad de la información provenientes de las diferentes áreas: Compliance, IT, Performance, legal, etc.

- Realizar la transferencia documental del Archivo de Gestión al Archivo Central de manera oportuna y acorde a los lineamientos definidos para tal fin.

- Mantener actualizado el sitio de archivo digital en sharepoint subiendo directamente los archivos a su cargo que deben quedar almacenados allí

- Evitar realizar copias de información crítica o confidencial o mantenerlas a la vista en los escritorios.

7.2. Alta Dirección (AES Corporación)

Responsables de:

- Establecer los lineamientos necesarios para ser incluidos en las políticas y procedimientos referentes con la Gestión de la Información.

7.3. Líderes de Áreas (Gerentes y Directores)

- Cumplir y hacer cumplir esta política.
- Participar en el diligenciamiento y/o actualización de las Tablas de Retención Documental
- Indicar la clasificación o desclasificación de la información que produce

7.4. Líder de Gestión de la Información

7.4.1. Alineación y actualización de políticas corporativas y legislación local para garantizar el cumplimiento de las mismas.
7.4.2. Mantener actualizada la presente política, así como los manuales, procedimientos e instructivos derivados de la Gestión de la información.
7.4.3. Divulgar y socializar la política y procedimiento de Gestión de la Información.
7.4.4. Administrar el contrato de servicios de Gestión documental con proveedor competente para la prestación del servicio. Definir alcance, responsabilidades e indicadores de gestión que garanticen el cabal cumplimiento de la presente Política y los procedimientos administrativos definidos.
7.4.5. Monitorear y auditar el proceso de archivo físico y digitalizado.

8. Clasificación de la Información.

Acorde con la Política de Manejo de la Información de la SBU Andes y con los lineamientos de la ley 1712 de 2014, Art. 18 Ley de Transparencia, la información en AES Chivor debe ser clasificada bajo los siguientes criterios:

8.1. **Clasificada (Rojo):** Antes conocida como Confidencial o reservada, este tipo de información se debe catalogar porque es considerada como de alta sensibilidad y/o relevancia para la toma de decisiones estratégicas, o que sean de impacto financiero, potencial de fraude y/o requisitos legales para la organización. Este tipo de información normalmente está protegida y se prohíbe su divulgación. A modo de ejemplo, sin que éstos puedan considerarse taxativos: Informes de la Gerencia, documentación sobre estrategias, Planes de fusión y adquisición, Planificación de litigios incluye comunicaciones con abogados internos y externos, Planes de desarrollo de nuevas operaciones comerciales.

Se debe controlar el acceso a quienes deban conocer la información, y no se debe divulgar a toda la empresa ni a externos, debido a que se puede poner en riesgo la seguridad e interés de clientes, asociados y empleados. Incluye toda aquella información que puede presentar riesgos para la compañía, y cuyo acceso debe ser expresamente autorizado por el responsable, el que deberá necesariamente restringirlo a un grupo reducido de usuarios que la necesiten para el desarrollo de sus tareas habituales.

8.2. **Interna (Azul):** Información que, sin ser **clasificada**, se debe mantener dentro de la empresa y no debe estar disponible externamente, excepto a terceros involucrados en el tema o por requerimiento de autoridad legal. Ejemplo: Base de datos, expedientes de RRHH, Informes de contabilidad, Informes financieros o estados de cuentas, planos técnicos, programas de paradas de máquinas por mantenimiento, intranet, carteleras digitales, material de entrenamiento, etc.

8.3. **Pública (Verde)**: Corresponde a la información sin ninguna de las categorías anteriores y su divulgación no afecta en términos de imagen ni económicamente a la empresa. No es necesario establecer restricciones especiales, más allá de las recomendaciones sobre su buen uso y la conservación. Ejemplo: Nombre y número de identificador fiscal de la empresa, extranet, notas periodísticas, notas de prensa, etc.

9. Restricciones de acceso a la información.

El acceso a la información física o electrónica estará determinado por las

normas relacionadas con los permisos, niveles de acceso y las restricciones a empleados, contratistas y terceros que establezcan los Propietarios de la Información. Estos permisos y niveles de accesos se deben establecer en las TRD con sus anexos y en concordancia con la Política de Manejo de la información.

10. Eliminación de Información.

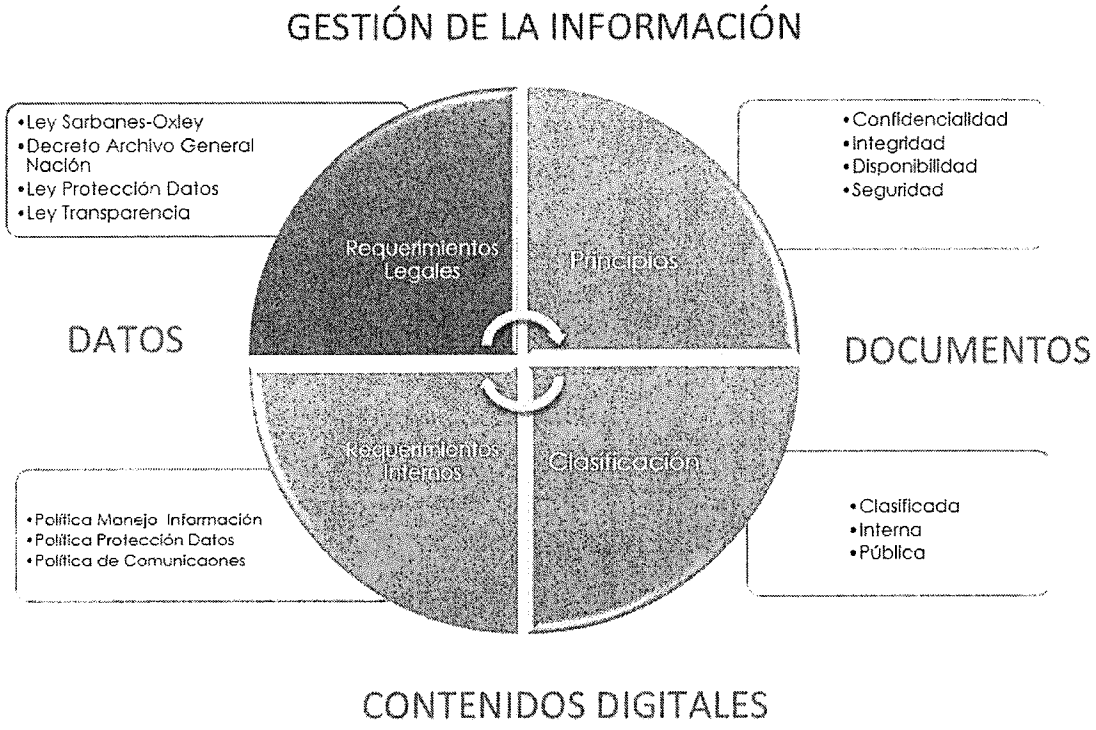
Los documentos físicos con información confidencial o reservada que requieran ser destruidos, deberán destruirse garantizando que sea imposible su recuperación, aplicando técnicas como el picado o triturado de papel.

El documento físico con información pública podrá ser eliminado bajo reciclaje.

En ningún caso la documentación podrá ser objeto de eliminación bajo incineración.

Todo medio informático de propiedad de AES Chivor (PC, Laptop, Memoria USB, Disco Duro, Tablet), deberá ser sometido a un proceso de borrado seguro de la información antes de su entrega o dada de baja, una vez se haya hecho backup de la información contenida y/o recuperada, de acuerdo a la Política de manejo de la información vigente.

Anexo 1


GESTIÓN DE LA INFORMACIÓN
•Ley Sarbanes-Oxley
•Decreto Archivo General Nación
•Ley Protección Datos
•Ley Transparencia
Requerimientos Legales
Principios
•Confidencialidad
•Integridad
•Disponibilidad
•Seguridad
DATOS
DOCUMENTOS
Requerimientos Internos
Clasificación
•Política Manejo Información
•Política Protección Datos
•Política de Comunicaones
•Clasificada
•Interna
•Pública
CONTENIDOS DIGITALES