TABLA DE CONTENIDO

1. OBJETIVO 2
2. CONDICIONES GENERALES 2
2.1 Alcance 2
2.2 Términos y definiciones 2
2.3 Documentos asociados 2
2.3.a Referencias normativas 2
3. DESARROLLO 3
3.1 Componentes de seguridad de la información 3
3.1.a Personas 3
3.1.b Tecnología 4
3.1.c Procesos 4
3.1.c.1. Ciclo de gestión segura de la información 4
3.1.c.1.1. Clasificación de la información 9
3.1.c.1.1.1. Información no confidencial 10
3.1.c.1.1.2. Información confidencialidad 11
3.1.c.1.1.3. Lineamientos de clasificación de la información 12
3.1.c.1.2. Tratamiento de la información 14
3.1.c.1.2.1. Rotulado de la información 14
3.1.c.1.2.2. Acceso a la Información Electrónica y Física 15
3.1.c.1.2.3. Identificación y aseguramiento de hojas electrónicas 16
3.1.c.1.2.4. Almacenamiento de la Información Electrónica y Física 16
3.1.c.1.2.5. Distribución y Transmisión de la Información 17
3.1.c.1.2.6. Disposición final y segura de la información 17
3.1.c.1.3. Análisis de riesgos 17
3.1.c.1.4. Implementación del Plan de Mitigación 17
3.1.c.1.5. Seguimiento 17
3.2 Responsabilidades De Los Usuarios Frente A La Información Y Los Recursos Tecnológicos 18
3.2.a Responsabilidades De Los Usuarios Frente a La Información Y Los Recursos Tecnológicos 18
3.2.a.1. Publicaciones Técnico Científicas 18
3.2.a.2. Derechos de Autor 18
3.3 Responsabilidad Legal y Consecuencias 18
4. CONTINGENCIAS 19
5. ANEXOS 19

Contenido de ilustraciones y tablas

Ilustración 1 - Modelo de apropiación de Ecopetrol S.A. 4
Ilustración 2 - Ciclo de gestión segura de la Información de Ecopetrol S.A 5
Ilustración 3 - Clasificación o categorización de la información 10
Ilustración 4 - Información clasificada o reservada, según la Ley de Transparencia 12
Ilustración 5 - Clasificación y etiquetado de la información medio digital 14

Tabla 1 - Algunos medios donde se puede presentar, almacenar o transferir la Información 5
Tabla 2 - Matriz de Roles y Responsabilidades en el Ciclo de Gestión Segura de la Información 8
Tabla 3 - Documento en construcción es Confidencial 13

1. OBJETIVO

Presentar los lineamientos de gestión en materia de Seguridad de la Información con referencia a las reglamentaciones aplicables y estándares adoptados en Ecopetrol S.A., con el fin de establecer los principios, criterios, responsabilidades, conductas y prácticas requeridas para la protección de los activos de información, promoviendo su adecuado tratamiento y buscando la reducción de exposición al riesgo fuga o pérdida. Esto basado en los lineamientos de los códigos de Ética y buen Gobierno de la Empresa.

2. CONDICIONES GENERALES

2.1 Alcance

Estos lineamientos aplican a Ecopetrol S.A. y contratistas que tengan acceso a información de Ecopetrol. Para las empresas del Grupo Empresarial este manual puede ser tomado como referencia.

2.2 Términos y definiciones

Delito Informático: delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación, etc.) y el creciente número de usuarios, consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión.

Cifrado: El cifrado es un método de protección de datos que consiste en alterarlos hasta hacerlos ilegibles. Los datos pasan de ser texto sin formato a ser texto cifrado por medio de un método denominado algoritmo. Quien desee acceder a los datos cifrados debe descodificarlos primero con la clave de descifrado correcta.

Data Lost Prevention: DLP o prevención de pérdida de datos es un conjunto de herramientas y procesos que se utilizan para garantizar que los datos confidenciales no se pierdan, se usen indebidamente o los usuarios no autorizados accedan a ellos.

https://ecopetrol.sharepoint.com/teams/gentepila/glosariocorpo/SitePages/Glosario.aspx.

2.3 Documentos asociados

2.3.a Referencias normativas

Interna:

- Circular responsabilidad en el uso de la información.
- Manual para el tratamiento de datos personales en Ecopetrol S.A.
- Guía de seguridad para sistemas y servicios informáticos.
- Guía para el uso adecuado del correo electrónico.
- Guía De Operación Para Líderes Funcionales Y/O Ejecutores De Controles De Los Sistemas de Información.

Externa:

- Constitución Política de Colombia de 1991, Artículo 15.
- Ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales".
- Ley 1712 del 6 de marzo de 2014, Ley de transparencia y del derecho de acceso a la Información pública nacional.
- Ley 1915 del 12 de julio de 2018, ley de derechos de autor y propiedad intelectual
- Artículo 269F de la Ley 1273 de 2009, Delitos informáticos.
- Artículo 34, numeral 5 de la Ley 734 de 2002 Código Disciplinario Único para Servidores Públicos.
- Decreto 1008 Sobre Política de Gobierno Digital
- Ley Sarbanes-Oxley Act of 2002 – Sección 404
- Resolución 500 de 2021, establece los lineamientos y estándares para la estrategia de seguridad digital.
- Ley 1952 de 2019 - Código General Disciplinario
- Ley 527 de 1999 - Comercio electrónico y mensajes de datos
- Ley 599 de 2000 - Código Penal Colombiano

3. DESARROLLO

3.1 Componentes de seguridad de la información

3.1.a Personas

Las personas y sus comportamientos frente al tratamiento de la información son un factor crítico para preservar su confidencialidad, integridad y disponibilidad.

El modelo de seguridad de la información en Ecopetrol S.A., trabaja con las personas en la sensibilización e interiorización de prácticas y comportamientos de protección y aseguramiento de la información.

Los funcionarios, colaboradores, contratistas, aliados, proveedores, grupos de interés, filiales y asociadas deben mantenerse informados y sensibles para adoptar comportamientos que protejan la información, de tal forma que se minimicen los riesgos de fuga o pérdida de información. Estos comportamientos son de dos tipos: el primero son los hábitos, es decir, las acciones "mecánicas" que se ejecutan para proteger la Información (por ejemplo: bloquear la sesión del computador cuando se ausenta del puesto de trabajo); y el segundo tipo se refiere a los comportamientos que requieren un nivel de conocimiento previo para ejecutarlo (por ejemplo: conocer el proceso de realización de copias de respaldo).

Se ha desarrollado el programa de concientización y apropiación de prácticas a través de las tres dimensiones del modelo de apropiación de Ecopetrol S.A.

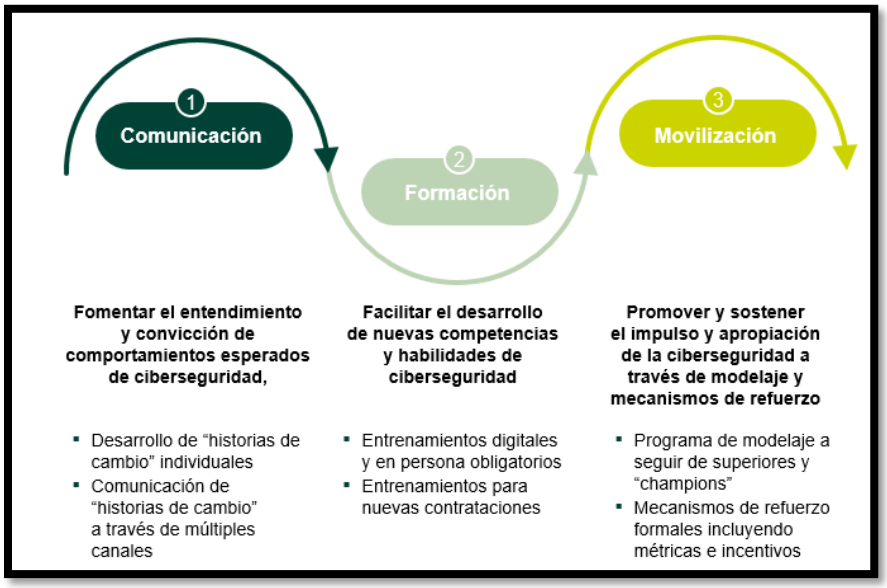

Ilustración 1 - Modelo de apropiación de Ecopetrol S.A.

3.1.b Tecnología

Ecopetrol S.A. cuenta con una serie de herramientas enfocadas en reducir o mitigar el riesgo de fuga y/o perdida de la información, por lo tanto, dependiendo de los análisis de riesgos que se hagan sobre las unidades de información críticas, se realizan instalaciones de herramientas para mitigar los riegos:

- Cifrado de Disco duro
- Cifrado de archivos
- Antivirus en equipos y en móviles
- Herramientas de Data Lost Prevention
- Control de contenido
- Otras

3.1.c Procesos

3.1.c.1. Ciclo de gestión segura de la información

La Información es un activo que tiene valor crítico y como tal debe ser divulgada y protegida dentro de los parámetros establecidos en la constitución política y la ley.

La Información relacionada con las actividades del negocio de la empresa debe ser clasificada de acuerdo con su fundamento de confidencialidad, tratada por las personas a cargo de ésta y eliminada cuando haya cumplido su propósito; lo anterior permite establecer mecanismos para la protección de la Información contra la pérdida, la destrucción, la divulgación no autorizada, acorde con los requisitos legales y de negocio.

La Información se almacena, presenta y transfiere en diferentes medios:

Medio	Ejemplos
Física	Documentos impresos
	Registros de investigación
	Fotografías
	Libros
Electrónica	Dispositivos móviles
	Equipos de cómputo
	USB y disco externo
	Videos
	Imágenes
	Mensajes de correo electrónico
	Archivos en diferentes formatos como Documentos, hojas electrónicas o presentaciones
	Servicios de almacenamiento en la nube
	Servicios de mensajería instantánea
	Sistemas de inteligencia artificial
	Redes sociales
Otros medios	Conocimiento de los funcionarios y contratistas
	Conversaciones
	Reuniones de trabajo

Tabla 1 - Algunos medios donde se puede presentar, almacenar o transferir la Información

A continuación, se diagrama el ciclo de gestión segura de la Información de Ecopetrol S.A., el cual permite orientar el adecuado manejo de la Información.

Ilustración 2 - Ciclo de gestión segura de la Información de Ecopetrol S.A

La Información pasa por diferentes etapas desde el instante en que se genera o se adquiere, hasta el momento de su disposición final. Es importante que, independientemente del medio en el que se encuentre, la información debe ser debidamente tratada y protegida.

Para Ecopetrol S.A. el Ciclo de Gestión Segura de la Información se establece teniendo en cuenta las siguientes etapas:

a) **Clasificación**: Ecopetrol S.A. adopta el fundamento de confidencialidad para la clasificación. Para desarrollar esta etapa se deben ejecutar dos actividades así:
   a. Identificación de las Unidades de Información: Consiste en listar las Unidades de Información del Proceso seleccionado de acuerdo con una fuente definida.
   b. Clasificación de la Información: Consiste en aplicar los criterios definidos en este manual para valorar a las unidades previamente identificadas.

b) **Análisis de Riesgos**: Consiste en la identificación del nivel de exposición al riesgo de Fuga o Pérdida de la Información utilizando la metodología de análisis de riesgos de Ecopetrol S.A. y formular las acciones de tratamiento requeridas para la mitigación del riesgo.

c) **Tratamiento**: La Información de Ecopetrol S.A. debe ser debidamente protegida de acceso no autorizado, modificación, transmisión o disposición final, sin importar el medio en el que se encuentre; se deben definir acciones de tratamiento para gestionar la Información en los siguientes momentos: Rotulado, Acceso, Transporte, Almacenamiento y Disposición final segura. Ver numeral 5.1.b.1.2. - tratamiento de la Información de este manual.

d) **Implementación del plan de tratamiento**: Consiste en implementar las acciones generales definidas en el plan de tratamiento. Esta implementación es responsabilidad del área dueña de la Información y debe seguir un cronograma previamente establecido donde se identifiquen los responsables y las fechas de inicio y finalización.

e) **Seguimiento**: Consiste en la medición post de la efectividad y sostenibilidad de las acciones del plan de mitigación implementadas.

Durante la ejecución del ciclo de gestión segura existen diferentes roles que intervienen en las actividades específicas que componen cada etapa. Las responsabilidades de cada rol frente a dichas actividades se han plasmado en una matriz RACI descrita en la tabla 2 y la descripción de cada rol se menciona a continuación:

Responsable de la Información: Se establece como responsable de la Información, al ejecutivo o dueño del proceso donde la misma se generó, obtuvo, adquirió, transformó o controló, bien sea por intermedio de funcionarios de Ecopetrol S.A o por personal contratista que soporte al proceso. Sus responsabilidades respecto de la información son:

- Su responsabilidad es controlar la generación, clasificación, tratamiento y protección adecuada de la Información.
- Clasificar y revisar periódicamente la Información, siguiendo los lineamientos definidos y establecer los planes de tratamiento acordes con dicha Información.
- Administrar y tratar la Información de acuerdo con su calificación, valor y criticidad.
- Establecer los usuarios que dentro de su área podrán tener acceso a la Información y los privilegios para su Tratamiento, así como verificar de manera periódica las restricciones de acceso y niveles de calificación de la Información, alineado con la normativa de Seguridad de la Información y Privacidad de Ecopetrol S.A.
- Asegurar el archivo del Documento que contiene la Información calificada acorde con las normas documentales vigentes.
- Asegurar que se cumplan las acciones de gestión del riesgo, para preservar la confidencialidad, la integridad y la disponibilidad de la Información.

- Mantener y revisar periódicamente la efectividad de las medidas de seguridad apropiadas en concordancia con la normativa vigente para la protección de la Información física y electrónica.

Usuario de la Información: Es el funcionario de Ecopetrol S.A. o la persona natural o jurídica contratista que haya sido autorizada por el Responsable de la Información para el Tratamiento de la misma. Dicho Tratamiento debe hacerse de acuerdo con las facultades definidas expresamente por el Responsable de la Información.

El Usuario de la Información tiene la responsabilidad de:

- Conocer los criterios de calificación de la Información de acuerdo con los parámetros definidos en el ítem 5.1.b.1.1 Clasificación de la Información.
- Apoyar a los Propietarios de la Información en la determinación de los requerimientos de protección y mecanismos de control de cada categoría de calificación.
- Tratar la misma preservando su calificación, de acuerdo con las obligaciones y/o funciones contractuales o legales.
- Asegurar su uso acorde con el Fundamento de Confidencialidad y realizar las acciones necesarias para mantenerla en el nivel en que ha sido calificada.

Custodio de la Información: Es el área de Ecopetrol S.A. que tiene el archivo y vigilancia de la Información generada por las áreas que puede estar este en medio físico o digital.

Tanto el responsable, el Usuario, como el Custodio de la Información deben estar atentos para identificar y reportar cualquier incumplimiento de las normas y procedimientos de Seguridad de la Información establecidos por la entidad.

Asesor Jurídico: Es el funcionario de Ecopetrol S.A. o persona autorizada para emitir el concepto por el cual se fundamenta de manera constitucional o legal la motivación de la Información clasificada y/o reservada.

Gerente de Ciberseguridad y Ciberdefensa: Es el funcionario de Ecopetrol S.A. que lidera y define junto con su equipo de trabajo las directrices, lineamientos, procedimientos y guías que estipulan el adecuado tratamiento de la Información en Ecopetrol S.A. en cumplimiento de las normas y leyes que aplican.

Profesionales enlace: Contactos de las áreas que apoyan la identificación, valoración e implementación del plan de tratamiento definido.

	Actividad	Responsable de la información	Usuario de la información	Custodio de la información	Jurídico	Gerente de Ciberseguridad y Ciberdefensa	Profesionales enlace
Clasificación	Definir y divulgar los lineamientos relacionados con la gestión del riesgo de fuga o pérdida de información crítica	I				A, R	
	Capacitación en clasificación de la Información	I	I	I	I	A, R	R

	Actividad	Responsable de la información	Usuario de la información	Custodio de la información	Jurídico	Gerente de Ciberseguridad y Ciberdefensa	Profesionales enlace
	Identificación y listado de unidades de Información	R, A	C, I	C, I	I	C, I	R
	Realizar clasificación de las unidades de información	R, A	C, I	C, I	I	C, I	R
	Verificar la motivación y emitir concepto jurídico, si aplica	A	C, I	C, I	R	I, R	
	Formalizar las unidades de información a la Vicepresidencia de Ciencia, Tecnología e innovación	R					R
Tratamiento	Elaboración de Plan de Tratamiento Estándar	C, A	C	C		I, R	
	Validación y aprobación del Plan de Tratamiento propuesto	R, A	I	I		I, C	R
	Ejecución Plan de Tratamiento Estándar	A, R	R	R		I, R	R
Análisis de Riesgos	Entregar Información verbal o escrita solicitada para la elaboración del análisis de riesgos	A, R	C	C		I	R
	Documentar y ejecutar el análisis de riesgos	A	I, C	I, C		C, R	
	Elaborar plan de mitigación de acuerdo con el análisis de riesgo y a las actividades estándar iniciales e incorporar al informe	C, I	I	I		A, R	R
	Oficializar el informe final de análisis de riesgos y plan de tratamiento.	R	C	C		A, I	R
Implementación plan de tratamiento	Ejecutar plan de mitigación	A, R	R	I		I, R	R
	Monitoreo al plan de mitigación y plan de trabajo	A	I	I		I, R	
Seguimiento	Planeación del seguimiento	I, C	I, C	I, C		A, R	R
	Ejecución del seguimiento	C, I, A	I, C	I, C		I, R	R
	Elaboración y entrega de resultados de seguimiento	I	I	I		A, R	R

Tabla 2 - Matriz de Roles y Responsabilidades en el Ciclo de Gestión Segura de la Información

3.1.c.1.1. Clasificación de la información

La seguridad de la información consiste en la preservación de los siguientes criterios de la información que se gestiona en los sistemas y procesos implicados en su tratamiento y a cargo de las personas que los operan al interior de Ecopetrol S.A., bien sean funcionarios o contratistas. La triada de seguridad de la información se describe a continuación:

- **Confidencialidad**: Consiste en proteger la información contra la visualización, divulgación o cualquier otro acceso no autorizado. La información confidencial debe ser protegida mediante mecanismos idóneos de procesos, personas y de herramientas (tecnológicas u otras aplicables a soportes físicos). Su acceso debe ser limitado, habilitándolo sólo a aquellos individuos que en realidad necesitan esa información para realizar sus tareas ("need to know basis"). Si se afecta la confidencialidad (por ejemplo, mediante divulgación o acceso no autorizado), se puede generar impactos negativos para la compañía.

- **Integridad**: La Información de Ecopetrol S.A. debe ser precisa, coherente y completa desde su creación hasta su disposición final y únicamente podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la Información puede exponer a la Empresa a toma de decisiones incorrectas y ocasionar fallas en los procesos, pérdidas financieras o afectación de la imagen.

- **Disponibilidad**: La Información debe estar en el momento, en el medio y formato que se requiera, al igual que los recursos necesarios para su uso. La no disponibilidad de la Información puede resultar en fallas en los procesos, pérdidas financieras y de imagen de la Empresa.

La categorización de la información se efectúa bajo un enfoque de confidencialidad. Al categorizar la información a su cargo, **cada área separa la información confidencial de aquella que no lo es**, para el efecto, Ecopetrol S.A. ha venido empleando como criterio orientador el previsto en la Ley de Transparencia y de Acceso a la Información[1]. Ésta norma define que las entidades pueden negar el acceso que les llegue a ser solicitado a información **clasificada, reservada[2]** y a **documentos en construcción[3]**. Además, la Corte Constitucional precisó que, tratándose de empresas en las que el Estado tiene participación, "…en relación con su actividad propia, industrial o comercial, no están en deber de información con respecto a dicha actividad."[4]. Por lo tanto, la categorización de información que hace cada una de las áreas respecto de la información a su cargo, es el punto de partida para proteger la información confidencial.

[1] Ley 1712 de 2014 o aquella que la modifique o sustituya.
[2] Ley 1712 de 2014, artículos 6 (literales c, d y e), 18 y 19
[3] *"Documento en construcción: No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio* (sic) *de un sujeto obligado en su calidad de tal".* Ley 1712 de 2014, artículo 6 (literal k).
[4] Sentencia C-734 de 2013, numeral quinto de la parte resolutiva

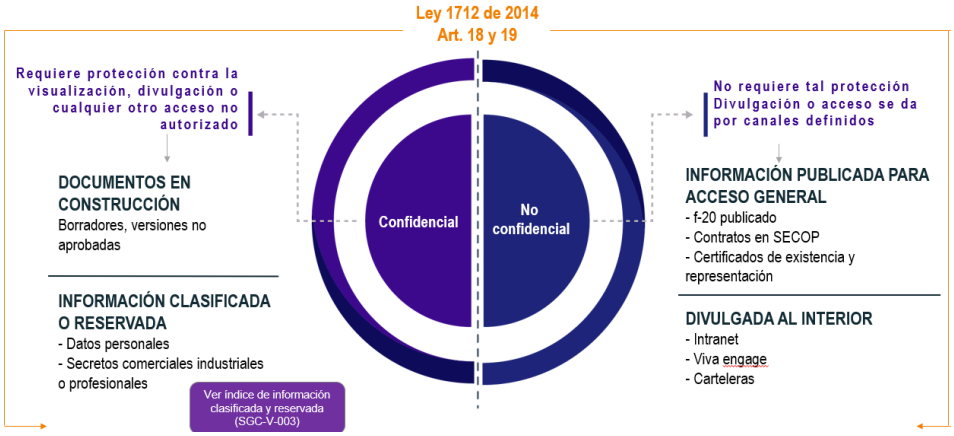

Ilustración 3 - Clasificación o categorización de la información

3.1.c.1.1.1. Información no confidencial

Existen múltiples razones por las cuales cierta información de Ecopetrol tenga vocación de ser pública y por lo tanto su carácter es opuesto al de aquella que se considera confidencial.

- Éstas pueden incluir obligaciones normativas derivadas de su carácter de sociedad de economía mixta. Por ejemplo, aspectos de transparencia y acceso a información pública sobre la entidad (ej. página web de la entidad), aspectos de contratación (por ejemplo, SECOP, cuando aplica), aspectos regulatorios aplicables a la actividad de la entidad (ej. reglas de publicidad de la Agencia Nacional de Hidrocarburos u otras entidades), entre otros.
- Otros aspectos obligatorios pueden derivarse de su carácter de emisor de valores, en Colombia o en la Bolsa de Valores de Nueva York. Esto incluye por ejemplo la presentación de informes financieros (ej. F20) o revelación de información relevante.
- Igualmente, hay información propia de las operaciones o iniciativas de la compañía, que tiene vocación de ser conocida por diferentes grupos de interés. Por ejemplo, convocatorias al programa de Bachilleres Ecopetrol, retos de innovación abierta, entre otras.
- Hay información que hace parte de la estrategia de comunicaciones de la compañía u otros anuncios dirigidos al público, en su portal web, sus redes sociales, entre otros.

Pese a que la información tenga la vocación de ser pública, su divulgación debe ser efectuada por los canales definidos para el efecto, según el proceso respectivo. A título simplemente ilustrativo, está el **Procedimiento para Divulgación de Información Relevante y no Relevante**, la **Guía corporativa para la gestión de comunicaciones del Grupo Ecopetrol** o algunas reglas del proceso de abastecimiento sobre publicación el **Sistema Electrónico para la Contratación Pública**. Por lo tanto, hasta que el área encargada autorice y/o efectúe la publicación respectiva, se trata de documentos en construcción.

a) Información pública o publicada para acceso general

Existe información que por ley es pública o reposa en fuentes de acceso público. Por ejemplo, los datos de identificación de la sociedad y sus representantes se encuentran en el certificado de existencia y representación de la compañía, que administra la Cámara de Comercio. La Ley de Transparencia define "publicar o divulgar" como "poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión".

Ante una solicitud de acceso a información que está disponible en fuentes de acceso abierto (cuya publicación ha sido autorizada por el área competente), el área a cargo podrá indicar que la información ya es pública e indicar al solicitante como acceder a la misma (ej. suministrando el enlace respectivo, cuando así aplique).

b) Información divulgada al interior de la compañía

La tabla 3 reseña algunos ejemplos de información divulgada al interior de la empresa. A éstos puede sumarse información en carteleras físicas, información presentada en charlas o capacitaciones, presenciales o virtuales, entre otros espacios con vocación de divulgación interna.

- Aunque se trate de información no confidencial, no se habilita la distribución abierta e indiscriminada del contenido.
- Tenga en cuenta que puede haber aspectos de comunicaciones, imagen, derechos de divulgación, entre otros aspectos que son pertinentes.
- El alcance de divulgación de la información es definido por las áreas a cargo de las comunicaciones o de la información respectiva, por lo que son quienes determinan si esta puede ser publicada externamente.

3.1.c.1.1.2. Información confidencial

Como se indicó anteriormente, categorizar información como confidencial requiere contar con el sustento respectivo.

a) Documentos en construcción

Allí se enunció por ejemplo que la Ley de Transparencia señala que los documentos en construcción no son considerados información pública. Salvo que el área encargada autorice publicarlos o compartirlos, podrán invocar este sustento legal para proteger la confidencialidad de tal información, por ejemplo, de cara a solicitudes de acceso o iniciativas de divulgación (Ver tabla 3).

b) Información clasificada o reservada

La Ley de Transparencia permite la protección de información clasificada o reservada. Como se enunció, su acceso puede ser negado de forma motivada, al amparo de las causales previstas en tales normas. Sobre esta base, las áreas han construido el **índice de información clasificada y reservada** reseñado en este documento. Allí, las áreas señalan las disposiciones normativas que sustentan esa categorización de la información.

Por lo tanto, con base en la ley y apoyada en el referente práctico de dicho índice u otros instrumentos de gestión documental, el área a cargo de la información respectiva puede sustentar el carácter confidencial de la información que corresponda a estas categorías.

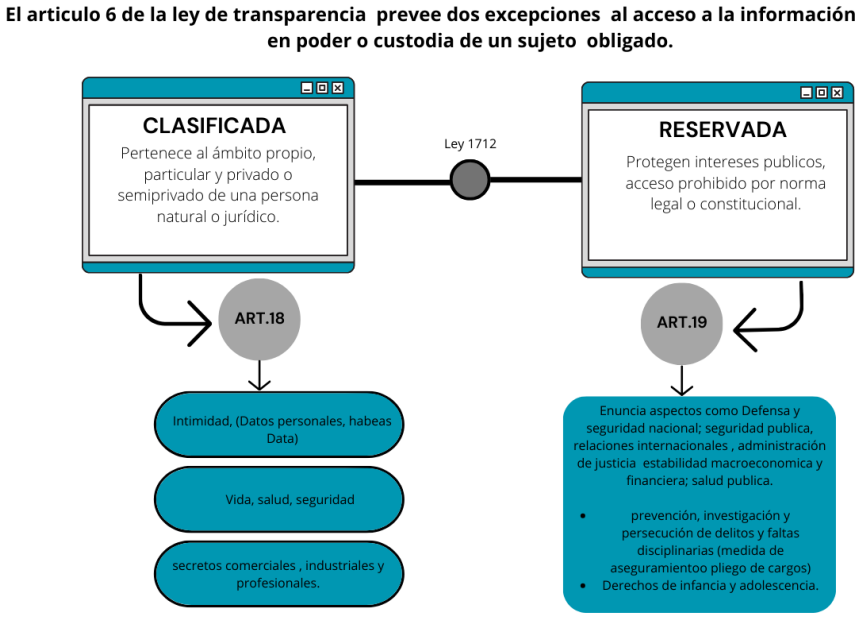

Ilustración 4 - Información clasificada o reservada, según la Ley de Transparencia

Tratándose, por ejemplo, de la protección al derecho a la intimidad, las normas resaltan que el acceso a datos personales requiere autorización del titular de la información o que concurra alguna de las excepciones consagradas en los artículos 6 y 10 de la Ley 1581 de 2012. En el mismo sentido, existe información asociada a la protección de información clasificada por su carácter de ser comercial, industrial o profesional. De la misma forma, arriba se reseñó que la Corte Constitucional (Sentencia C-734 de 2013) definió precisiones al alcance de publicidad en entidades con participación estatal, tratándose de temas asociados a la actividad propia, industrial o comercial.

Dada la multiplicidad de tipos documentales y procesos que se gestionan al interior de Ecopetrol, cada área tiene la responsabilidad de categorizar la información que corresponda a estas categorías. Según las particularidades de cada temática, en algunos casos se denominará por ejemplo información privilegiada, con un sustento del régimen financiero pertinente. En otros se trata por ejemplo de reserva de historia clínica. En trámites disciplinarios, la reserva procesal correspondiente. Cada área desde el dominio del tema a cargo sustenta la confidencialidad para categorizar la información a su cargo y protegerla adecuadamente.

3.1.c.1.1.3. Lineamientos de clasificación de la información

- Al categorizar la información, el área a cargo debe establecer si la información es o no confidencial.

- En caso de serlo, el área debe hacer el análisis y tener el sustento respectivo.
- El índice de Información Clasificada y Reservada y demás elementos asociados de gestión documental son referentes que las áreas deben mantener actualizados. Por lo tanto, son referentes de consulta al momento de categorizar determinada información.
- Dada la gran variedad de temáticas y tipologías de información que gestiona Ecopetrol, el análisis de cada área es determinante, a la luz de las reglas que rigen sus actividades y procesos. Éstas pueden involucrar incluso aspectos temporales cuando son determinantes para la confidencialidad.

Escenario teórico	Aspecto temporal	Sustento de confidencialidad
Información que tiene vocación de ser pública (ej. comunicado o texto de información relevante)	Suponga que el documento está en fase de elaboración y validación interna (borrador)	Documento en construcción Ley 1712 de 2014, artículo 6 (literal k).

Tabla 3 - Documento en construcción es Confidencial

- Existe información de la compañía que, por disposición normativa o decisión de la empresa, tiene vocación de ser divulgada.
- Al analizar si la información es o no confidencial, valide si se trata de información pública (o que deba tener ese carácter) o si ya está publicada para acceso general.
- La publicación y forma de divulgación de información debe ser autorizada siguiendo las reglas que apliquen (ver, por ejemplo, el **Procedimiento para Divulgación de Información Relevante y no Relevante**).
- Para clasificar la información en medio digital se deben usar las herramientas de clasificación y etiquetado definida por la organización (confidencialidad - sensibilidad) dispuesta en la suite office 365, de la siguiente manera:

a) Información no confidencial:

Etiqueta: ECP-NO CONFIDENCIAL
Subetiqueta: ECP – publica (Información pública o publicada para acceso general)
Subetiqueta: ECP – Divulgación interna (Información divulgada al interior de la compañía)

b) Información confidencial

Etiqueta: ECP - Confidencial
Subetiqueta: ECP información en construcción
Subetiqueta: ECP información clasificada y/o reservada

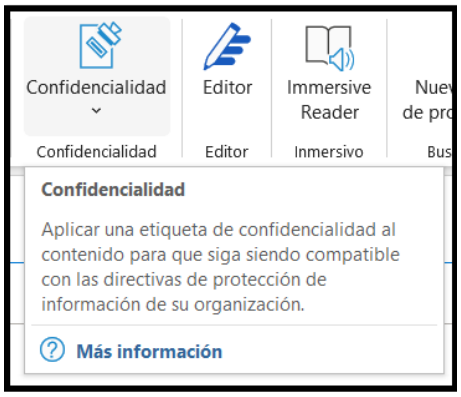

Ilustración 5 - Clasificación y etiquetado de la información medio digital

3.1.c.1.1.4. Lineamientos de clasificación en correo electrónico

- Para mensajes de correo electrónico, estos deben incluir en la parte inferior, después de la firma, las leyendas (disclaimers automáticos) tanto en español como en inglés que se describe en la guía para el uso adecuado del correo electrónico

- Para los mensajes de correo electrónico estos deben estar etiquetados de acuerdo con la evaluación de confidencialidad.

- Cuando se necesite de canales de transmisión de alta seguridad, se debe hacer uso de la herramienta de transferencia segura de archivos dispuesta por la organización

3.1.c.1.2. Tratamiento de la información

El tratamiento de la Información hace referencia a las actividades que las personas ejecutan con la Información. Algunas de estas acciones sin limitarse a ellas son: Rotulado, Acceso, Almacenamiento, Distribución, Transmisión y Disposición final, las cuales se van a tratar a continuación, de acuerdo con el nivel de confidencialidad definido por Ecopetrol S.A.

3.1.c.1.2.1. Rotulado de la información

Como resultado de la calificación de la Información el área/proceso da un nivel de confidencialidad alto, el rotulado de la Información se debe realizar de la siguiente manera:

- **Para documentos en papel**, se rotularán como "CONFIDENCIAL" o "NO CONFIDENCIAL" y se podrán realizar con sello o se deben marcar con tinta que no pueda ser borrada fácilmente en la margen superior central de la hoja; para los casos en que el documento tenga más de una hoja, se debe especificar el número total de folios que lo componen, igualmente se marcará la última página en blanco si llegase a aplicar.

Cuando los documentos contengan Información relacionada con la intimidad, la salud o la seguridad de las personas, clasificados como "CONFIDENCIAL" se podrán rotular como "DATO PERSONAL".

- **Para los documentos electrónicos** deben ser etiquetados con el grado de confidencialidad correspondiente que asignará automáticamente una marca de agua o pie de página. No deben existir copias no controladas de los documentos con clasificación de información "CONFIDENCIAL".

- **Para dispositivos de almacenamiento** como CDs, DVDs, entre otros, que requieran ser marcados con algún tipo de tinta indeleble, se debe colocar el título de la Información que contenga y el rótulo "CONFIDENCIAL" o "NO CONFIDENCIAL", según sea el caso.

3.1.c.1.2.2. Acceso a la Información Electrónica y Física

- Las personas que accedan a Información "CONFIDENCIAL" deben contar con la autorización del responsable de la Información.

- Los funcionarios o colaboradores que traten la Información que sea "CONFIDENCIAL", deben contar con acuerdos de confidencialidad vigentes.

- El acceso a la Información que ha sido clasificada y rotulada como: "CONFIDENCIAL", debe limitarse a aquellos funcionarios o terceros debidamente autorizados por la Empresa para cumplir con sus responsabilidades laborales y/o contractuales.

- El líder del área/proceso debere solicitar a quien administre los sitios y de manera periódica (de acuerdo con las necesidades del área o como mínimo cada tres meses) una relación de los usuarios que tienen permiso a las carpetas donde se almacena Información "CONFIDENCIAL" y así validar frente a los usuarios permitidos y notificar al servicio si existe alguna modificación para mantenerla actualizada. Adicionalmente se deben verificar otros sitios y aplicaciones corporativas, tales como, SharePoint, OpenTex, entre otras.

- Para el acceso a la información registrada en los sistemas y procesos de información, se debe atender lo establecido en los documentos, en particular los lineamientos, responsabilidades y prácticas de control:

    - Guía Para la Gestión Integrada de Riesgos en el Grupo Ecopetrol
    - Guía De Operación Para Lideres Funcionales y/o Ejecutores De Controles De Los Sistemas De Información.
    - Guía Para la Gestión de Segregación de Funciones en los Sistemas de Información

- La Consulta y préstamo de documentos y expedientes de archivos generados (no importando si es electrónico o físico) en las áreas/procesos archivados y custodiados en los Archivos de Gestión y en el Archivo Central de Ecopetrol S.A., deben seguir los lineamientos del "Instructivo para la consulta y préstamo de documentos y expedientes".

- Para el acceso a los archivos de Gestión y Archivo Central, se deben verificar las personas autorizadas para acceder a la Información "CONFIDENCIAL" y cumplir con la normativa de Gestión Documental.

3.1.c.1.2.3. Identificación y aseguramiento de hojas electrónicas

- Las hojas electrónicas con información "CONFIDENCIAL" o con información de tipo personal que tengan impacto o no en los reportes financieros (SOX y no SOX) deben ser tratadas de acuerdo con el "***instructivo para la identificación y aseguramiento de hojas electrónicas con impacto en el reporte financiero"*, en el capítulo 3.3.2. Actividades de control sobre las hojas electrónicas.** Teniendo en cuenta los controles claves mencionados a continuación:

  - ✓ El dueño del proceso, dueño de la hoja y/o persona designada por el dueño de proceso, deben determinar un repositorio oficial donde guarden las hojas electrónicas (sharepoint/teams/otros).

  - ✓ Organizar las hojas electrónicas en una estructura de repositorio con acceso restringido a las personas que por sus funciones lo requieran (lectura, creación, modificación).

  - ✓ Revisar trimestralmente los usuarios con acceso a las hojas electrónicas y repositorio definido, para corroborar que tengan acceso únicamente los usuarios autorizados, de lo contrario debe solicitar la corrección de las excepciones identificadas.

  - ✓ Proteger las celdas formuladas de la hoja electrónica con el fin de prevenir la modificación no autorizada de la información contenida en esta

- Para las hojas electrónicas que contienen o gestionan información de tipo personal, se debe realizar el análisis de riesgos de flujos de información de acuerdo con el documento **Instructivo para la elaboración de análisis de riesgo de flujos de información** y validar la pertinencia de su reporte ante la SIC[5].

3.1.c.1.2.4. Almacenamiento de la Información Electrónica y Física

- La Información electrónica de carácter "CONFIDENCIAL" en cada área/proceso, debe guardarse en los repositorios corporativos destinados por la Empresa para tal fin y el Responsable de la Información debe revisar y actualizar periódicamente los permisos a dichos repositorios.

- Para el caso que la Información física necesite pasar a custodia del servicio de Archivo, cada propietario debe tener en cuenta los criterios definidos en las Tablas de Retención Documental (TRD) de la dependencia correspondiente, disponibles en repositorio oficial, así como también los permisos para su acceso.

[5] Superintendencia de industria y comercio

3.1.c.1.2.5. Distribución y Transmisión de la Información

- El Responsable de la Información, en el evento de efectuar una distribución y/o transmisión de Información, debe enviarla debidamente etiquetada o rotulada y dando a conocer a su destinatario sobre el tratamiento que este nivel de confidencialidad exige.

- Cuando se traten temas "CONFIDENCIALES" en reuniones entre funcionarios o entre funcionarios y terceras partes, se debe realizar teniendo en cuenta medios de comunicación seguros y autorizados por la Empresa.

- En el evento de compartir Información "CONFIDENCIAL" con un tercero, se debe consultar previamente con el apoyo jurídico del área para aclarar temas contractuales y los alcances de las leyes aplicables.

- Para los casos en los que se requiera COMPARTIR INFORMACIÓN (no importando el formato) "CONFIDENCIAL", se deben usar las herramientas colaborativas y seguras dispuestas por la organización.

3.1.c.1.2.6. Disposición final y segura de la información

- Para eliminar Información "CONFIDENCIAL" se debe tener autorización por escrito del jefe del área a la que pertenece el Responsable de la Información. El proceso de eliminación depende del medio de almacenamiento en el cual se encuentre (impreso o digital).

- La disposición final debe estar de acuerdo con tablas de retención documental y sus procedimientos correspondientes.

3.1.c.1.3. Análisis de riesgos

Consiste en la identificación del nivel de exposición al riesgo de ciberataques y fuga o pérdida de la Información utilizando la metodología de análisis de riesgos de Ecopetrol S.A.[6] y formular las acciones de tratamiento requeridas para la mitigación del riesgo. Durante esta etapa debe quedar definido completamente el plan de tratamiento que reúne las acciones requeridas producto de dicho análisis de riesgos y las acciones iniciales propuestas de acuerdo con el análisis realizado durante la etapa de tratamiento.

3.1.c.1.4. Implementación del plan de tratamiento

Consiste en implementar las acciones generales definidas en el plan de tratamiento. Esta implementación es responsabilidad del área dueña de la Información y debe seguir un cronograma previamente establecido donde se identifiquen los responsables y las fechas de inicio y finalización.

3.1.c.1.5. Seguimiento

Consiste en la verificación del cumplimiento de las de las acciones del plan de tratamiento definidas y se generan alertas en caso de que sea requerido.

[6] Matriz de Valoración de Riesgos Estratégicos - ECP-UGR-F-008

3.2 Responsabilidades de los Usuarios frente a la información y los recursos tecnológicos

Las tecnologías para la seguridad de información se articulan con las arquitecturas empresariales y cumplen su ciclo de vida, implementación, operación, mantenimiento y salida, de acuerdo con la estrategia que establece la Gerencia de Ciberseguridad y Ciberdefenda.

3.2.a Responsabilidades de los usuarios frente a la información y los recursos tecnológicos

La protección sobre la Información de Ecopetrol S.A. identificada como "CONFIDENCIAL" es responsabilidad de los funcionarios o contratistas que con ocasión de su cargo tienen acceso a la misma o la tienen bajo su cuidado.

3.2.a.1. Publicaciones Técnico Científicas

Para la realización de Publicaciones técnico-científicas, se debe dar cumplimiento a lo establecido en el procedimiento de publicaciones técnico-científicas vigente, estas deben contar con el aval de la autoridad técnica y del gerente del área correspondiente a su rol antes de su divulgación.

3.2.a.2. Derechos de Autor

Ecopetrol S.A. protege y exalta los Derechos de Autor tanto para las obras impresas como en la protección del Software que utilizan sus funcionarios y contratistas. Por ello, sin perjuicio de las obligaciones normativas sobre protección de derecho de autor, los siguientes son los lineamientos con relación a los derechos de autor:

1. Usar únicamente software debidamente licenciado.
2. En presentaciones, documentos, informes y demás documentos que utilicen los funcionarios y/o contratistas para las labores de su cargo debe mencionarse la fuente de donde se extrajo la Información.
3. Abstenerse de realizar copias parciales o totales de libros, artículos, reportes y otros documentos; que no estén permitidos por la ley de derecho de autor.
4. La Información de Ecopetrol S.A. es propiedad de la Entidad, por lo cual, no puede ser utilizada para ningún fin diferente al establecido y requerido en la ejecución de las labores correspondientes a su cargo. Por lo tanto, no podrá ser utilizada como fuente de Información para temas promocionales, comerciales, entre otros.

3.3 Responsabilidad Legal y Consecuencias

Debido a que el uso inadecuado de los recursos de Ecopetrol S.A. puede causar fuga o pérdida de Información sensible de la entidad y ésta es considerada un activo de la compañía; su afectación en integridad, disponibilidad o confidencialidad puede considerarse como un evento de fraude, lo que conlleva consecuencias para la Entidad y para las personas involucradas en el hecho.

El incumplimiento de este manual podrá ser objeto de sanciones que pueden llegar hasta la terminación del contrato de trabajo en el caso de trabajadores, sin prejuicio de las acciones legales (penales, disciplinarias, civiles) a que haya lugar, según leyes aplicables vigentes. Para el caso de proveedores rigen las cláusulas establecidas en los contratos que median su relación con Ecopetrol S.A.

4. CONTINGENCIAS

N/A

5. ANEXOS

N/A

RELACIÓN DE VERSIONES

Documento Anterior			
Versión	**Fecha dd/mm/aaaa**	**Código y Título del Documento**	**Cambios**
1	14/04/2011	ECP-DTI-M-067 Manual de gestión segura de la información	Incorporada dentro del manual de seguridad de la información.
1	01/04/2012	PDO-G-001 Guía de uso adecuado de redes sociales	Incorporada dentro del manual de seguridad de la información.
2	31/05/2012	PDO-G-002 Guía de responsabilidad en el uso de dispositivos móviles	Incorporada dentro del manual de seguridad de la información.
2	09/10/2014	IDO-G-016 Guía para la clasificación de la información de Ecopetrol S.A. de acuerdo con su nivel de tratamiento.	Incorporada dentro del manual de seguridad de la información.
1	28/05/2015	PDO-I-028 Instructivo para proteger la información de Ecopetrol S.A.	Incorporada dentro del manual de seguridad de la información.
1	07/09/2015	PDO-G-005 Guía de responsabilidad de los usuarios en el acceso y uso de la información y de los recursos informáticos de Ecopetrol S.A.	Incorporada dentro del manual de seguridad de la información.
1	12/05/2016	PDO-M-011 Manual De Seguridad De La Información	Primera versión del documento
1	29/09/2023	SGY-M-002 - MANUAL DE SEGURIDAD DE LA INFORMACIÓN	Documento Nuevo
1	01/07/2020	SSI-M-00X - MANUAL DE SEGURIDAD DE LA INFORMACIÓN Actualización código Ajuste a la nueva estructura de la Gerencia GCY	

		Actualización de términos y tecnologías referidas Se incluyó la política de conexión de visitantes a red wifi ECP Se eliminó el numeral 3.3.g de "uso de medios de almacenamiento externo, debido a que se fue incluido en la guía SGY-G-002
1	17/11/2023	SGY-M-002 - MANUAL DE SEGURIDAD DE LA INFORMACIÓN Actualización código Ajuste a la nueva estructura de la Gerencia GCY Actualización de términos y tecnologías referidas Se incluyó la política de conexión de visitantes a red wifi ECP Se eliminó el numeral 3.3.g de "uso de medios de almacenamiento externo, debido a que se fue incluido en la guía SGY-G-002 Se incluyo en numeral 5.1.b.2.3 Distribución y Transmisión de la Información las herramientas de clasificación y etiquetado en el Office 365 Cambio de codificación y sistema de gestión.
Documento Nuevo		
Versión	**Fecha dd/mm/aaaa**	**Cambios**
2	20/06/2024	Actualización del capítulo de clasificación de la información y ajuste en lineamentos, inclusión de lineamientos de hojas electrónicas no SOX
3	20/06/2024	Inclusión de lineamientos de hojas electrónicas no SOX validado con gestión administrativa
4	31/07/2024	Actualización en taxonomía de etiquetas
5	08/11/2024	Actualización del capítulo 3.1.c.1.2.3 Identificación y aseguramiento de hojas electrónicas
6	06/12/2024	Actualización de la Etiqueta de Confidencialidad del este documento.

Para mayor información sobre este documento dirigirse a quien lo elaboró, en nombre de la dependencia responsable:

Elaboró: Daliris Milena Maldonado
Buzón: daliris.maldonado@ecopetrol.com.co
Dependencia: Vicepresidencia Ciencia Tecnología e Innovación

Revisó	Aprobó
ERICA ALEXANDRA REINA CEBALLOS Profesional de Ciberseguridad **Registro No. E0287174** Vicepresidencia De Ciencia Tecnología e Innovación	**ELKIN FERNEY QUINTERO GOMEZ** Gerente de Ciberseguridad y Ciberdefensa **Registro No.** E0307304 Vicepresidencia De Ciencia Tecnología e Innovación

*Documento firmado electrónicamente, de acuerdo con lo establecido en el **Decreto 2364 de 2012**, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.*

*Para verificar el cumplimiento de este mecanismo, el sistema genera un **reporte electrónico que evidencia la trazabilidad de las acciones** de revisión y aprobación por los responsables. Si requiere verificar esta información, solicite dicho reporte a Service Desk.*