TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

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 y el sistema de gestión de Ciberseguridad.

2. CONDICIONES GENERALES

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

- **Confidencialidad**: La Información debe ser accedida sólo por las personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la Información con confidencialidad alta puede implicar impactos en Ecopetrol S.A., en términos económicos y de imagen.

- **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.

3. DESARROLLO

3.1 Referencia Normativa

Interna:

- circular SSI-J-002 Ciberseguridad
- Circular responsabilidad en el uso de la información
- Manual para el tratamiento de datos personales en Ecopetrol S.A.
- Manual de Ciberseguridad Para Sistemas de Control y Automatización Industrial
- Guía de seguridad para sistemas y servicios informáticos
- Guía para el uso adecuado del correo electrónico
- Guía de gestión de riesgos y controles de seguridad de la información
- Guía De Operación Para Líderes Funcionales Y/O Ejecutores De Controles De Los Sistemas de Información

- Guía Para La Arquitectura Digital Objetivo Ecopetrol

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

3.2 Componentes De La Seguridad De La Información

3.2.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, trabaja con las personas en la sensibilización e interiorización de prácticas y comportamientos de protección y aseguramiento de la información.

Los funcionarios y colaboradores 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

Figura 1. Modelo de apropiación de Ecopetrol

3.2.b **Procesos**

3.2.b.1. Ciclo De Gestión Segura De La Información De Ecopetrol S.A.

La Información es un activo que tiene valor crítico y como tal debe ser divulgada y protegida[1] 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:

[1] ISO 27001- objetivos de control y controles, numeral A.7.2 –Clasificación de la información

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

Medio	Ejemplos
Física	Documentos impresos
	Registros de investigación
	Fotografías
	Libros
	Microfichas
Electrónica	Dispositivos móviles
	Equipos de cómputo
	USB y disco externo
	CDs ó DVDs
	Videos
	Imágenes
	Mensajes de correo electrónico
	Archivos en diferentes formatos como Documentos, hojas electrónicas o presentaciones
Otros medios	Conocimiento de los funcionarios y contratistas
	Conversaciones
	Reuniones de trabajo

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.

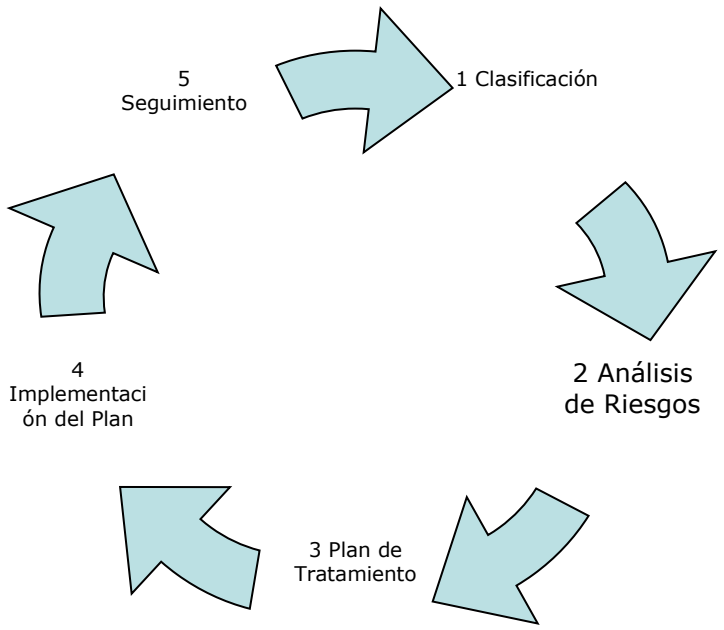

Figura 2. Ciclo de gestión segura de la Información de Ecopetrol S.A

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 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 a 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.[2] 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 3.2.b.1.2. - tratamiento de la Información* de este manual.

d) Implementación del Plan de Mitigación: 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 3 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.

2 Matriz de Valoración de Riesgos Estratégicos - ECP-UGR-F-008

- 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 *3.2.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 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 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.

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

	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
	Identificación y listado de unidades de Información.	R- A	C-I	C-I	I	C-I	R
	Realizar clasificación de las Unidades.	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 VDI.	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 al 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 el plan de mitigación	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

R (Responsable) **A** (Accountable) **C** (Consultado) **I** (Informado)

3.2.b.1.1. Clasificación de la Información

Para una correcta clasificación de la Información se debe utilizar el Fundamento de Confidencialidad, con el fin de que ésta sea tratada por las personas, de acuerdo con el rol que desempeñan en la Empresa, sea conocida solo por la autoridad que en ejercicio de sus funciones o disposición legal pueda tener acceso a ella y, en general, por toda persona, con sujeción a los límites constitucionales y legales.

La clasificación de la Información se enmarca dentro de dos grandes grupos como se menciona a continuación:

Confidencialidad Baja

La Información que se encuentra en este nivel de confidencialidad corresponde a las categorías de **PUBLICADA Y GENERAL.**

PUBLICADA para efectos de este manual, es toda Información que haya sido suministrada al público en general, a través de los medios de comunicación oficiales de Ecopetrol S.A., por Comunicaciones Corporativas en medios masivos de comunicación o entregada para su publicación a las autoridades que ejercen su supervisión. Este tipo de Información requiere medidas mínimas de protección frente a su aspecto de integridad (modificaciones no autorizadas), para efectos de este manual, como ejemplos de la Información que se puede clasificar como PUBLICADA se tienen:

- Los boletines de prensa publicados por Ecopetrol S.A.
- Los estados financieros luego de haber sido aprobados y publicados.

- La información que de Ecopetrol S.A. reposa en las páginas oficiales de los entes de vigilancia y control.
- Información publicada en la página web de Ecopetrol S.A.
- Información mínima obligatoria que debe publicarse acorde con los lineamientos de Gobierno en Línea (GEL).

GENERAL es toda Información que circula libremente dentro de Ecopetrol S.A., que es propia de su quehacer y su revelación no autorizada no compromete el buen nombre de la empresa y no afecta en ninguna proporción las relaciones con terceros o grupos de interés. Algunos ejemplos de Información que se puede clasificar como GENERAL son:

- Información de la Intranet de Ecopetrol.
- Videos institucionales.
- Información que se publica en las carteleras y en medios tales como la red social empresarial de Ecopetrol S.A "Yammer".

Por lo anterior la Información que se encuentre clasificada con nivel de confidencialidad bajo **no se rotula**.

Confidencialidad Alta

Es aquella Información que no debe circular más allá de las personas que están autorizadas a conocerla. Su revelación no autorizada puede comprometer la viabilidad de la empresa como sociedad de economía mixta, los derechos de terceros y la seguridad, entre otros, pudiéndose:

- ➔ Afectar la posición competitiva de Ecopetrol S.A. frente a los particulares, en desarrollo de su objeto social, al generar incumplimiento de normas o acuerdos de voluntad, afectar las relaciones o negociaciones con los grupos de interés o la imagen y el buen nombre de la empresa, a nivel nacional o internacional.
- ➔ Afectar el curso de las investigaciones preliminares de los entes de control.
- ➔ Afectar el debido proceso y demás garantías procesales.
- ➔ Afectar la posición competitiva de Ecopetrol S.A. frente a los particulares, en desarrollo de su objeto social, al generar incumplimiento de normas o acuerdos de voluntad.
- ➔ Contrariar las disposiciones constitucionales o legales, aplicables a la Información reservada o limitada por aquellas.
- ➔ Comprometer operaciones o actividades de negocio[3].
- ➔ Comprometer la seguridad nacional o pública.
- ➔ Constituir un secreto comercial, industrial o profesional.
- ➔ Poner el riesgo la vida, intimidad, seguridad o salud de las personas.

La Información que se encuentra en este nivel de confidencialidad, corresponde a las categorías **CLASIFICADA** ó **RESERVADA.**

CLASIFICADA es la Información que estando en poder o custodia de un sujeto obligado en su calidad tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica,

[3] Artículo 7 de decreto 1056 de 1953

por lo que su acceso podrá ser negado o exceptuado[4]. Esta negación o rechazo debe ser de **manera motivada y por escrito**, siempre que el acceso pudiere causar un daño a los siguientes derechos[5]:

a) El derecho de toda persona a la intimidad, a la Información personal no pública, protegida por el derecho al habeas data.
b) El derecho de toda persona a la vida, la salud o la seguridad;
c) Los secretos comerciales, empresariales[6], industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011.

La Información que cumpla con los criterios mencionados anteriormente, debe ser rotulada como **CLASIFICADA.**

Ejemplos de Información CLASIFICADA son:

- Líneas sísmicas en los procesos exploratorios.
- La Información técnica y científica respecto de prospectos de yacimientos obtenidos directamente por Ecopetrol S.A. o por sus asociadas.
- La Información originada en comités Directivo y de Negocios.
- El informe técnico de producción de pozos.
- Actas del Comité Directivo.
- El inventario de tanques de almacenamiento de crudos.
- El inventario de sistemas de Información de la empresa.
- Actas con el resultado de los procesos de selección.
- Valor de negociaciones de crudo con cada uno de los clientes.
- Datos personales, tales como:
    - Origen racial.
    - Filiación política.
    - Orientación política.
    - Condiciones religiosas.
    - Datos de Salud.
    - Número de teléfono de la residencia.
    - Dirección de residencia.
    - Afiliación a Sindicatos.

RESERVADA es la Información que estando en poder o custodia de un sujeto obligado en su calidad tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos[7]. Esta negación o rechazo debe ser de **manera motivada y por escrito**, siempre que el acceso estuviere expresamente prohibido por una norma legal o constitucional[8]:

a) La defensa y seguridad nacional.
b) La seguridad pública.
c) Las relaciones internacionales.
d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.

[4] Literal C articulo 6 ley 1712 de 2014
[5] Articulo 18 ley 1712 de 2014
[6] Secreto empresarial, el artículo 260 de la decisión 486 de 2000 establece el régimen común de propiedad intelectual.
[7] Literal d) artículo 6 ley 1712 de 2014
[8] Artículo 19 ley 1712 de 2014

e) El debido proceso y la igualdad de las partes en los procesos judiciales.
f) La administración efectiva de la justicia.
g) Los derechos de la infancia y la adolescencia.
h) La estabilidad macroeconómica y financiera del país.
i) La salud pública.

La Información que cumpla con los criterios mencionados anteriormente, debe ser rotulada como **RESERVADA**.

Ejemplos de Información RESERVADA:

- Expedientes disciplinarios hasta la formulación del pliego de cargos.
- Los convenios con la fuerza pública.
- Información relevante que ha sido sometida a reserva acorde con las normas de mercado de valores.

Dado que la Información con confidencialidad alta no puede circular más allá de las personas que por su cargo o rol están autorizadas a conocerla, es decir sólo fluye dentro de un proceso especifico y definido, si no está en uso debe mantenerse guardada bajo llave (si es física) o con control de acceso (si es electrónica o digital).

En caso de que la Información CLASIFICADA y RESERVADA sea solicitada por terceros, su acceso podrá ser denegado siempre que se motiven las circunstancias legítimas y necesarias y puedan verse afectados los derechos mencionados anteriormente, en los cuales se base la excepción al acceso de este tipo de Información.

A continuación se resume la clasificación de la Información, según su nivel de confidencialidad:

Tabla 3. Clasificación de la información

Nivel de Confidencialidad	Ley 1712 de 2014	Clasificación Ecopetrol	Criterios para clasificar	¿Cómo se puede obtener? Por terceros
Bajo	Información Pública	Publicada	➔ No tiene afectación para la Empresa.	➔ Sin reserva alguna.
		General	➔ No compromete el buen nombre de la empresa. ➔ No afecta en ninguna proporción las relaciones con terceros o grupos de interés.	➔ Con previa autorización del dueño del proceso o área
Alto			➔ Poner en riesgo Información personal no pública, protegida por el derecho al habeas data. ➔ Poner en riesgo la vida, la intimidad, la seguridad o la	➔ Por orden de autoridad administrativa en ejercicio de las funciones legalmente asignadas.

	Información Pública Clasificada	Clasificada	salud de las personas. ➔ Constituir un secreto comercial[9], empresarial, industrial, profesional o de otro tipo previsto en la ley.	➔ Por solicitud del causahabiente o apoderado del titular de los Datos Personales. ➔ A las entidades públicas o administrativas en ejercicio de sus funciones legales [10] ➔ Por orden judicial.
Alto	Información Pública Reservada	Reservada	Pueda afectar: ➔ La defensa y seguridad nacional. ➔ La seguridad pública. ➔ Las relaciones internacionales. ➔ La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso. ➔ El debido proceso y la igualdad de las partes en los procesos judiciales. ➔ La administración efectiva de la justicia. ➔ Los derechos de la infancia y la adolescencia. ➔ La estabilidad macroeconómica y financiera del país. ➔ La salud pública. ➔ Afectar las relaciones o negociaciones con los grupos de interés o la imagen y el buen nombre de la empresa.	➔ Solo Puede ser obtenida por orden de autoridad competente en cumplimiento de funciones legalmente asignadas. Nota: El acceso podrá ser rechazado o denegado de manera motivada y por escrito siempre y cuando estuviese expresamente prohibido por una norma legal o constitucional.

[9] Matriz de Valoración de Riesgos Estratégicos - ECP-UGR-F-008
[10] Acorde con la sentencia C-748 de 2011 para la entrega de esa información a la autoridad debe haber quedado demostrado para Ecopetrol (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información.

3.2.b.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.:

3.2.b.2. Rotulado de la Información

Como resultado de la calificación de la Información en 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 "INFORMACIÓN CLASIFICADA" o "INFORMACIÓN RESERVADA" y se podrán realizar con sello o se deberán 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 deberá 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 "CLASIFICADA" se podrán rotular como "DATO PERSONAL".

- Al realizar la distribución o envío de Información Clasificada vía correo electrónico, en el campo "Asunto:" se debe incluir "***INFORMACIÓN CLASIFICADA***", "***INFORMACIÓN RESERVADA***" o "***DATO PERSONAL***" seguido del tema del cual trata el correo.

- **Para los documentos electrónicos** se deberán rotular con marcas de agua, buscando que no interfieran con la legibilidad de los mismos, ni en su original ni al momento de ser digitalizado o fotocopiado, es importante resaltar que no deben existir copias no controladas de los documentos con nivel de confidencialidad alto.

- Para dispositivos de almacenamiento como CDs, DVDs o cintas, entre otros, que requieran ser marcados con algún tipo de tinta indeleble, se deberá colocar el título de la Información que contenga y el rótulo "CLASIFICADA", "RESERVADA" o "DATO PERSONAL", según sea el caso.

Por otra parte, si como resultado de la clasificación de la Información en el área/proceso se obtiene un nivel de confidencialidad bajo, es decir, Información GENERAL o PUBLICADA, esta **NO REQUIERE** ser rotulada. Este tipo de información requiere medidas mínimas de protección frente a su aspecto de integridad (modificaciones no autorizadas).

Tabla 4. Rotulado de Información

Nivel de Confidencialidad	Clasificación	Rótulo
Bajo	Publicada General	Sin rótulo
Alto	Clasificada [11](se debe motivar cada una de las clasificaciones)	CLASIFICADA
	Reservada (se debe motivar cada una de las clasificaciones)	RESERVADA

3.2.b.2.1. Acceso a la Información Electrónica y Física

Las personas que accedan a Información del nivel alto de confidencialidad deberán contar con la autorización[12] del Responsable de la Información.

Los funcionarios o colaboradores que traten la Información que sea clasificada en el nivel alto de confidencialidad, deben contar con acuerdos de confidencialidad vigentes[13].

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

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".

El líder del área/proceso deberá solicitar periódicamente (de acuerdo con las necesidades del área o como mínimo cada tres meses) a la Mesa de Ayuda una relación de los usuarios que tienen permiso a las carpetas donde se almacena Información "CLASIFICADA" o "RESERVADA", validar[14] 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, P8, entre otras.

Para el acceso a los archivos de Gestión y Archivo Central, se deben verificar las personas autorizadas para acceder a la Información del nivel alto de clasificación y cumplir con la normativa de Gestión Documental.

[11] Para efectos de dato personal se puede rotular la información como DATO PERSONAL
[12] Se recomienda que la autorización se realice y documente por medio electrónico.
[13] Consultar el AC general de la Compañía o consultar el apoyo jurídico disponible en el área.
[14] Cada área deberá notificar a los usuarios registrados si aún requiere el acceso a la carpeta indicada, si no se obtiene respuesta en una semana a partir de la notificación inicial, por parte de los usuarios mencionados, el dueño de la carpeta procederá a revocar los permisos de acceso.

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

- Guía de gestión de riesgos y controles de seguridad de la información
- Guía de operación para los líderes funcionales de los sistemas de información
- Guía de Segregación de Funciones en los Sistemas de Información.

3.2.b.2.2. Almacenamiento de la Información Electrónica y Física

La Información contenida en dispositivos de almacenamiento como computadores portátiles o discos duros que sea de carácter CLASIFICADA O RESERVADA Ó DATO PERSONAL deberá estar cifrada con la herramienta dispuesta por la empresa para cifrado de disco duro para hacerlo cada funcionario deberá solicitar al Service desk el servicio de instalación de esta herramienta. Asimismo, la Información en formato físico con este nivel de confidencialidad deberá ser resguardada en lugar seguro bajo llave y no podrá ser conocida por personas que no estén autorizadas por el Responsable de la Información. Adicionalmente se deben contemplar los otros medios disponibles en el momento o los que aparezcan nuevos.

La Información electrónica con nivel de confidencialidad alto en cada área/proceso, deberá guardarse en los repositorios corporativos destinados por la Empresa para tal fin y el Responsable de la Información deberá 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 deberá tener en cuenta los criterios definidos en las Tablas de Retención Documental (TRD) de la dependencia correspondiente, disponibles en repositorio oficial P8, así como también los permisos para su acceso.

3.2.b.2.3. Distribución y Transmisión de la Información

Se debe contar con permiso del Responsable de la Información (escrito o por correo electrónico) para ser transmitida y/o transportada dentro y fuera de las instalaciones, independientemente si se encuentra impresa o de forma electrónica.

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

Cuando se traten temas Reservados y/o Clasificados en reuniones entre funcionarios o entre funcionarios y terceras partes, se deberá realizar de manera preferente en las instalaciones de Ecopetrol o los sitios autorizados por Seguridad Física, y siempre teniendo en cuenta medios de comunicación seguros y autorizados por la Empresa.

En el evento de compartir Información "CLASIFICADA", "RESERVADA" y/o "DATO PERSONAL" con un tercero, se deberá consultar previamente con el apoyo jurídico del área para aclarar temas contractuales y los alcances de las leyes aplicables.

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

Cuando el correo es transmitido a través de buzones externos, se deben cumplir las siguientes indicaciones:

- No deberá mencionar en ninguna parte su nivel de confidencialidad.
- No deberá dar detalles de la Información adjunta.
- Deberá usar la herramienta de cifrado de correo, para lo cual debe seguir las siguientes instrucciones:
    - Coloque en el asunto las palabras CIFRADO HES ASUNTO
    - Envíe el correo con el adjunto de manera normal
    - Cuando el correo llegue al destinario, se verá una leyenda que indica que el correo es Privado y Confidencial.
    - Para abrirlo deberá seguir las instrucciones del mensaje que consiste en descargar los adjuntos, crear una cuenta y la activación de la misma se enviará al mismo correo con el fin de validar su autenticación.

Cuando se necesite de canales de transmisión de alta seguridad, se deben considerar protocolos como HTTPS, SSL, TLS, entre otros. Para estos efectos, se debe consultar al Service desk.

Para los casos en los que se requiera COMPARTIR INFORMACIÓN (no importando el formato) "CLASIFICADA" o "RESERVADA", se deberán usar SFTP y seguir las siguientes instrucciones:

- Realizar el listado o inventario de los archivos con su extensión, nombre, fecha de creación, tamaños y su clasificación que debe ser firmado por la persona encargada o responsable de la Información y debe hacer parte de la documentación entregada al tercero.
- Utilizar las herramientas autorizadas por la Compañía para cifrar la Información, asignando una contraseña de acceso.
- Marcar (Rotular) el medio de almacenamiento seleccionado de acuerdo con el nivel de confidencialidad definido.
- Enviar en dos correos electrónicos diferentes la contraseña de la Información cifrada, a la persona que el tercero o el solicitante ha previsto para trabajar la Información, puede ser otro mecanismo, como un link a un sitio web con la contraseña a compartir.

En el caso de que la Información "CLASIFICADA" o "RESERVADA", requiera ser enviada a otras dependencias de Ecopetrol S.A., o entre ciudades, se debe utilizar el servicio de correo certificado 4-72.

A manera de resumen se ilustra en la tabla 5 los mecanismos de seguridad requeridos según su nivel de calificación.

Tabla 5.Mecanismos de seguridad según la calificación de la Información

NIVEL DE CALIFICACIÓN	MECANISMOS DE SEGURIDAD	CRITERIO DE SEGURIDAD		
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
GENERAL Y PUBLICADA	N/A		X	
CLASIFICADA	CONTROL DE ACCESO	X	X	X
RESERVADA	CONTROL DE ACCESO + CIFRADO	X	X	X
PROPIEDAD INTELECTUAL SECRETO COMERCIAL	CONTROL DE ACCESO + CIFRADO + DOBLE AUTENTICACIÓN	X	X	X

El MFA (Múltiple Factor de Autenticación) se trata de una medida de seguridad adicional, que requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder al servicio.

3.2.b.2.4. Disposición Final Segura de la Información

Una vez se ha determinado que la Información ha cumplido su función u objetivo, se debe proceder a eliminarla o depurarla de forma segura del medio que la contiene, de tal manera que los residuos magnéticos, ópticos, electrónicos o cualquier otra representación de los datos que han sido borrados, no sean recuperables[15].

Para eliminar Información con confidencialidad ALTA 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, el cual puede ser impreso o digital.

Se reitera que esta eliminación de la Información es distinta de la eliminación o disposición de documentos de archivo definidos en las tablas de retención documental.

3.2.b.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.[16] 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

[15] NIST 800-88. Guidelines for media Sanitization
16 Matriz de Valoración de Riesgos Estratégicos - ECP-UGR-F-008

riesgos y las acciones iniciales propuestas de acuerdo a análisis realizado durante la etapa de tratamiento.

3.2.b.4. Implementación del Plan de Mitigación

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.

3.2.b.5. Seguimiento

Consiste en la medición posterior sobre la efectividad y sostenibilidad de las acciones del plan de mitigación implementadas.

3.2.c Tecnología

Ecopetrol 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

Las tecnologías para la seguridad de información se articulan con las Arquitecturas empresariales y cumplen su ciclo de ruta, implementación, operación, mantenimiento y salida, de acuerdo con la Estrategia que establece la Gerencia de Ciberseguridad.

3.3 Responsabilidades De Los Usuarios Frente A La Información Y Los Recursos Tecnológicos

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

3.3.a Control de Acceso de los Aplicativos

Las personas que accedan a la Información, deben tener en cuenta las consideraciones generales para el acceso, descritas en el literal *b. Acceso a la Información Electrónica y Física* del ítem *3.2.b.2.1 Tratamiento de la Información,* además de tener en cuenta la *gestión de contraseñas*, descrita en el literal *2.2.b de la guía de Seguridad para Sistemas y Servicios Informáticos.*

3.3.b Acceso a la Red interna y Conexiones externas

Los siguientes lineamientos deben ser tomados en consideración con el propósito de utilizar la red corporativa de Ecopetrol S.A., tanto alambrada como inalámbrica, diseñada para proveer los medios de comunicación necesarios para que los funcionarios y contratistas puedan adelantar sus labores encomendadas en condiciones de seguridad:

- Todo equipo de cómputo que requiera acceso a la red interna de Ecopetrol S.A., deberá tener como mínimo las siguientes medidas de seguridad: Solución antimalware instalada y actualizada, parches de seguridad al día y mecanismo de autenticación habilitado para el ingreso al equipo.
- Abstenerse de ingresar a la red corporativa con una identidad diferente a la propia.
- Abstenerse de monitorear el tráfico de red, excepto cuando éste se encuentre debidamente autorizado por la Coordinación de Seguridad Informática.
- Abstenerse de adicionar elementos de cómputo y de red no autorizados, como enrutadores inalámbricos, switches, módems, etc.
- Abstenerse de compartir los recursos de la estación de trabajo (carpetas, archivos, unidades entre otros) con otros usuarios de la red interna o fuera de ella.
- Utilizar los sistemas de almacenamiento corporativos para compartir archivos con otro usuario dentro de la red de Ecopetrol S.A asegurando los accesos y permisos según corresponda.

Dada la sensibilidad de la Información que se almacena tanto en los servidores corporativos como en las estaciones de trabajo, el acceso a la red corporativa desde el exterior es controlado. Estas conexiones externas deberán ser solicitadas y justificadas ante el Service desk para su revisión y aprobación y pueden darse siempre y cuando cumplan con los siguientes requisitos:

- El funcionario que usará este medio de comunicación debe contar con la aprobación de su jefe o superior inmediato.
- El funcionario que ingrese a la red corporativa debe identificarse y autenticarse adecuadamente.
- El intercambiado de Información se encuentre cifrado.

Si la conexión es con un socio de negocios de Ecopetrol S.A. a través de internet, se deben utilizar los medios oficiales de conexión establecidos por la Vicepresidencia digital.

Los proveedores de aplicaciones o equipos informáticos que requieran conectarse a la red de datos de Ecopetrol S.A. para prestar algún tipo de servicio deben utilizar únicamente los mecanismos oficiales dispuestos para tal efecto. El acceso de estos proveedores a la red de la Entidad debe estar restringido únicamente a los recursos a intervenir, por un tiempo limitado y contar con la autorización expresa del administrador del contrato.

3.3.b.1 Conexión de visitantes mediante red WIFI

Ecopetrol habilita a los visitantes de sus instalaciones el acceso a la red de visitantes de internet a través de WiFi, el cual permite conectar usuarios simultáneamente mediante equipos como computadores, tablets, smartphones, celulares, entre otros, para facilitar la necesidad de interacciones

que se generan en las instalaciones y en algunas ubicaciones de atención al público, cumpliendo las siguientes obligaciones normativas:[17]

- Al acceder y utilizar la red de WIFI de Ecopetrol, el visitante declara que ha leído, entendido y acepta los términos y condiciones para su utilización. Si el visitante no está de acuerdo con esta normatividad no podrá acceder a este servicio.

- Los visitantes son responsables de configurar los dispositivos con los procedimientos básicos para el funcionamiento dentro de la red inalámbrica y de acuerdo protocolo creado para el efecto.

- Los visitantes se comprometen a hacer uso productivo y seguro de la red inalámbrica, según los niveles de acceso a Internet establecidos por Ecopetrol.

El visitante al hacer uso de la red Wifi está estrictamente prohibido:

- El uso para generar ganancias monetarias personales o propósitos comerciales.
- Transmitir y/o distribuir cualquier material que viole la ley o regulación de derechos de autor u otros derechos de propiedad intelectual, como software sin licencia, música, videos, películas, entre otros.
- Revelar o ceder las credenciales de autenticación de la red inalámbrica a personal no autorizado.
- Descargar servicios broadcast como audio y video.
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico.
- Instalar o realizar labores de recolección o escucha de información en tránsito por la red.
- Instalar equipos y/o software que genere interrupción o interferencia con la emisión normal de la red inalámbrica.
- Violar derechos de propiedad intelectual de Ecopetrol o de cualquier tercero.
- Afectar de cualquier manera el funcionamiento de redes o servicios, incluyendo, sin limitarse a afectaciones a sistemas de ciberseguridad y funcionamiento de operaciones digitales.
- Acceso no autorizado a los sistemas de información o de operación.
- Adelantar acciones de intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades, ataques de denegación de servicios, phishing o cualquier otra acción que afecte directa o indirectamente los sistemas, o constituya una actuación ilegal.
- Cargar o usar archivos que contengan virus, software malicioso, malware, generadores de fishing, gusanos informáticos, o herramientas o prácticas similares.
- Obtener información de los usuarios de Internet para fines comerciales no autorizados previamente, mediante publicidad engañosa o artilugios de cualquier índole, divulgarla o ponerla a disposición de entidades o procesos no autorizados.
- Afectar la privacidad de las comunicaciones o la intimidad de otros usuarios.
- Generar acciones de engaño, suplantación, inducción a error o cualquier otra que tenga el potencial de afectar derechos de terceros.

[17] Por ejemplo, la Resolución 3436 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones.

- Monitorear el tráfico de la Red de Visitantes u otras redes asociadas.
- Realizar alguna acción establecida en la Ley 1273 de 2009 – Ley de delitos informáticos.
- Es responsabilidad de los usuarios contar con el software y configuración de seguridad en su equipo personal para minimizar el riesgo al que se puede ver expuesto a un ataque informático al encontrarse conectado sobre esta red.
- De ninguna forma ni caso específico Ecopetrol será responsable por cualquier daño que pueda sufrir el equipo o dispositivo personal usado para establecer conexión a la red inalámbrica.
- El usuario es responsable de toda actividad que se lleve desde su equipo o dispositivo mientras esté conectado a la red inalámbrica.
- Es responsabilidad del usuario la seguridad física del equipo o dispositivo, Ecopetrol no es responsable por robo o daños al equipo del usuario. El usuario acepta y reconoce que Ecopetrol sólo provee el servicio de acceso a internet.

3.3.c Uso del correo electrónico corporativo

Tenga en cuenta los lineamientos frente al uso de su cuenta de correo electrónico corporativa en el documento: **Guía Para el Uso Adecuado del Correo Electrónico** publicado en normativa corporativa.

3.3.d Uso adecuado de Redes sociales

Los lineamientos dispuestos a continuación, aplican a todos los colaboradores de Ecopetrol S.A., incluyendo a aquellos que están facultados para representar a la compañía en las redes sociales. Asimismo, aplica a aquellos usuarios que hagan referencia a Ecopetrol S.A. a título personal en alguna de ellas.

- Como medida de prevención y para evitar posibles infecciones de virus o software malicioso, el acceso a las redes sociales debe realizarse desde equipos cuyo antivirus se encuentre actualizado a la fecha del ingreso a la red social.
- El contenido publicado por la Entidad y asociado a esta marca en las redes sociales no podrá contener:
  - Información cuyo nivel de confidencialidad haya sido clasificado por el Propietario de la misma como CLASIFICADA o RESERVADA.
  - Información ofensiva o racista.
  - Ataques personales, insultos o lenguaje amenazante.
  - Declaraciones difamatorias.
  - Información protegida con derechos reservados de autor.
  - Información personal o privada publicada sin consentimiento.
  - Información con mensajes políticos.
  - Información personal o privada publicada sin consentimiento.
  - Información promocional, salvo aquella que la Gerencia de Comunicaciones Corporativas autorice.
  - Fotos, imágenes o videos que se pueden clasificar en cualquiera de las anteriores categorías.

- Cuando se utilicen las redes sociales a título personal, debe dejarse en claro que las expresiones, discusiones u opiniones son de quien las expresa y no se emiten a título de la Entidad.

- Si un funcionario o contratista publica contenidos en las redes sociales asociado de alguna manera con las actividades adelantadas al interior de Ecopetrol S.A., debe adicionar el siguiente mensaje en español y en inglés:

  "Las publicaciones realizadas en este sitio representan el punto de vista del autor y no constituyen una opinión, posición oficial o estratégica de Ecopetrol S.A.

  The postings on this site are my own and don't necessarily represent Ecopetrol S.A.'s positions, strategies, or opinions."

- En los sitios de las redes sociales en las que Ecopetrol S.A. hace presencia, solo el área de Comunicaciones Corporativas es la encargada de hacer la publicación oficial.

  Los colaboradores que administran el contenido de dichos sitios, deben identificar la clasificación de la Información antes de ser publicada; para los casos donde identifiquen algún grado de confidencialidad en la Información o cuando se trata de publicar opiniones que definan la posición de la empresa frente a un tema, deberán contar previamente con la autorización escrita del área de la Empresa que genera o procesa dicha Información y la previa aprobación del contenido a publicar por parte de la Gerencia de Comunicaciones Corporativas. En ninguna red social está permitido publicar Información clasificada al interior de Ecopetrol S.A. como CLASIFICADA o RESERVADA, ya que se debe tener en cuenta que lo que se publica en estos sitios estará disponible al público por un periodo largo de tiempo.

- Los colaboradores que realicen publicaciones en las redes sociales a nombre de Ecopetrol S.A. deben contar previamente con la autorización escrita de su superior inmediato y la previa aprobación del contenido por parte de la Gerencia de Comunicaciones Corporativas.

  De igual manera, si los colaboradores desean participar en los diferentes foros, deberán tener en cuenta las siguientes recomendaciones:

  - Identificarse con su nombre, indicar que trabajan para la Entidad y mencionar su rol o cargo dentro de Ecopetrol S.A.
  - Publicar únicamente aquella Información cuyo nivel de confidencialidad es bajo, es decir PUBLICADA.
  - Preservar el nivel de confidencialidad de la Información que está a su cargo.
  - Mantener atención a las discusiones o participaciones.
  - Separar las opiniones de los hechos.
  - Respetar la audiencia y a los colaboradores que estén participando en la red social.
  - Usar tono cálido en los aportes.
  - Respetar las leyes de derecho de autor.
  - Corregir los errores inmediatamente, si se comente alguno.
  - Dar valor a las discusiones.

- Los colaboradores de Ecopetrol S.A. no pueden usar la identidad de otro funcionario de la Entidad o de alguna de sus filiales dentro de las redes sociales.

- No está autorizado el uso de logos, palabras u otras marcas en las redes sociales en las cuales se sube Información a nombre de Ecopetrol S.A., en donde se pueda infringir una marca registrada o cualquier otro tipo de propiedad intelectual, sin el permiso expreso del dueño de dicha marca.

- Se considera adecuado realizar publicaciones en redes sociales desde los equipos de cómputo de la Entidad por el personal autorizado para ello, siempre que estén relacionadas con las labores que se adelantan al interior de Ecopetrol S.A. y cumplan con los lineamientos expresados en el presente Manual.

- Con respecto al acceso a las redes sociales desde equipos de uso personal, los colaboradores deben tener en cuenta:

    - Cuando sus comentarios se relacionen explicita o tácitamente con Ecopetrol S.A., aclarar que su posición es personal y no corporativa.
    - No está autorizado el usar redes sociales para comentar, divulgar o publicar Información clasificada al interior de la Entidad como CLASIFICADA o RESERVADA.
    - Practique comportamientos seguros cuando publique y comparta Información personal para evitar ser víctima de los delincuentes informáticos. Dentro de estos comportamientos seguros se tiene:

        - ✓ Nunca publique:
            - La dirección de la casa ni el teléfono.
            - El número de cédula, fecha de nacimiento.
            - El lugar de trabajo.
            - El nombre del colegio de los niños.
            - Fotos de la casa, el carro, la placa.
            - Planes de vacaciones.
        - ✓ Revise el perfil ¿cómo quiere que lo vean los demás? y la configuración de privacidad.
        - ✓ Piense bien antes de publicar fotografías.
        - ✓ Acepte como amigos a personas que realmente conozca.
        - ✓ Revise la Información de sus hijos, el perfil, los amigos, con quiénes comparte fotos.

- Mantenga actualizado su antivirus para evitar ataques por software malicioso.
- Los siguientes son comportamientos apropiados para hacer uso adecuado de las redes sociales:

    - Indique claramente que los comentarios expuestos en las redes sociales son suyos y no involucran la posición de la Entidad, a menos que por las funciones de su cargo deba hacer publicaciones en nombre de Ecopetrol S.A.
    - Evite divulgar mediante las redes sociales Información indebida, ilegal, pornográfica o racista o cualquier otra que se considere contraria al debido respeto a sus compañeros de trabajo, amigos o competidores.
    - Absténgase de utilizar lenguaje que sea ofensivo, obsceno, insultante o difamatorio.

- Cuide la Información escrita o audiovisual que publica y comparte en las redes sociales, ya que estas pueden ser malinterpretadas por otros y generar malestar a los demás.
- Proteja su privacidad utilizando las herramientas que ofrecen las redes sociales para custodiarla; sólo acepte como amigos a aquellas personas que en realidad conoce.
- Recuerde cumplir con todas las leyes aplicables, como las de derechos de autor y protección de datos.
- Recuerde que los comportamientos éticos y morales en las redes sociales son iguales a los que posee en la vida real: ellos no son negociables.

3.3.e Uso de Internet

Internet es servicio que facilita Ecopetrol S.A. a sus funcionarios y contratistas para adelantar exclusivamente las labores propias de sus cargos y debe ser utilizado de manera austera y eficiente. Por ello, los siguientes son los lineamientos del buen uso de este servicio:

1. Utilizarlo únicamente para los servicios de navegación y transferencia de archivos autorizados.
2. Abstenerse de utilizarla para fines diferentes a los laborales, como, por ejemplo, comerciales o políticos.
3. Abstenerse de ejecutar herramientas de hacking, penetración o cualquier otra herramienta de seguridad desde Internet.
4. Abstenerse de colocar Información de Ecopetrol S.A. independientemente de su formato (Word, Excel, Power Point, pdf, avi, mp3, mp4 o cualquier otro formato actual o futuro) o su nivel de clasificación de confidencialidad (clasificada, reservada o de uso general) en sitios de internet o los denominados discos, carpetas virtuales o cualquier sistema de publicación de documentos, actual o futuro dentro o fuera de las instalaciones de Ecopetrol S.A.
5. Abstenerse de publicar material que pueda ser considerado como inapropiado, ofensivo, racial, sexual o irrespetuoso a otros, y de igual manera no acceda a dicho tipo de material.
6. Abstenerse de utilizar aplicaciones que permitan evadir los controles implementados por Ecopetrol S.A.
7. El acceso a páginas web con contenido inapropiado se encuentra restringido. Sin embargo y si por la naturaleza del cargo se requiere el acceso a páginas de acceso controlado, se debe solicitar a Service Desk su acceso adjuntando la aprobación y justificación por parte del jefe o superior inmediato.
8. El sistema de comunicaciones unificadas oficial de Ecopetrol S.A. será el establecido por la Vicepresidencia Digital. Este sistema de comunicaciones permite realizar videoconferencia, chat, reuniones de trabajo y llevar la extensión asignada fuera de la red interna de la Entidad para los funcionarios autorizados. Así las cosas, no está autorizado el uso de cualquier otro sistema de comunicaciones actual o futuro diferente a los ya establecidos por Ecopetrol.

3.3.f Uso de los Dispositivos Móviles

No se permite el transporte de Información CLASIFICADA y RESERVADA en dispositivos móviles. El colaborador es el responsable de la administración y debida eliminación de la Información en estos dispositivos.

Al usar medios como celulares, tabletas y demás tecnologías móviles se deben activar las opciones de geolocalización y de borrado remoto de la Información almacenada en el dispositivo en caso de robo o pérdida del mismo, si éste las soporta.

Se debe evitar el uso de este tipo de equipos en lugares públicos donde las personas alrededor puedan tener visibilidad de los datos trabajados o utilizar un filtro de privacidad que evite que se revele Información a personal no autorizado.

En caso de que el equipo soporte conexión vía bluetooth, se deben proteger estas conexiones mediante contraseña y haciendo que esta no se encuentre visible a todos los equipos.
Los usuarios son los responsables de asegurar el debido tratamiento, los niveles de seguridad y el adecuado acceso a la Información que almacenan y transportan en este tipo de medios. Por esto deben tomar todas las acciones preventivas necesarias para custodiar y proteger dicha Información, de manera que se evite que personas no autorizadas tengan acceso tanto a los dispositivos móviles como a la Información contenida en ellos, bien sea personal o corporativa.

Dentro de las acciones a tener en cuenta, están:

- Protección Física
  - No deje desatendido el dispositivo móvil en ningún momento.
  - Evite realizar o contestar llamadas en sitios públicos o en la calle si el dispositivo móvil tiene esta capacidad.
  - Avise de manera inmediata a las autoridades competentes sobre la pérdida o robo del dispositivo móvil. Así mismo y si el dispositivo tenía Información de Ecopetrol almacenada dentro de él, repórtelo como incidente de seguridad de la Información.

- Control de Acceso
  - Active las siguientes opciones de seguridad en el dispositivo móvil, si el mismo las soporta:
    - Proteja el dispositivo móvil contra accesos no autorizados mediante contraseña fuerte.
    - Active la opción de borrado seguro en el dispositivo móvil después de varios intentos fallidos de acceso.
    - Active la opción de bloqueo en el dispositivo móvil después de varios minutos de inactividad.
  - Tome medidas adicionales cuando digita la contraseña de acceso al dispositivo en lugares públicos, de manera que no exponga su contraseña ante terceros no autorizados.

- Uso de software licenciado o de origen conocido.
  - Instale y use software debidamente licenciado y de origen conocido, de manera que mitigue el riesgo de uso de software con código malicioso, que exponga la Información almacenada en los dispositivos móviles a fuga o pérdida de la Información.

- Uso de Antivirus y activación de Firewall Personales.
  - Instale antivirus para el dispositivo móvil que lo soporte y manténgalo actualizado. Así mismo, active el Firewall personal.

- Manejo de correo electrónico
  - Si va a intercambiar Información sensible de ECOPETROL S.A. a través de correo electrónico mediante un dispositivo móvil, cífrela.

- Active los servicios adicionales del dispositivo móvil solo cuando lo requiera.

- Evite conectarse a redes inalámbricas no conocidas.

- Mantenga el sistema operativo de su dispositivo móvil actualizado.

3.3.g Uso de Software legal

Los funcionarios de Ecopetrol S.A. solo podrán utilizar software legalmente adquirido y/o autorizado por la Entidad. Se puede hacer copia o duplicación de software licenciado por parte de los funcionarios, sólo cuando esta explícitamente permitido en los términos y condiciones de la licencia. Si un funcionario requiere instalar un software específico, debe tener la aprobación formal de la Vicepresidencia Digital, área que analizará las implicaciones a nivel de licencia y uso que este software pueda tener en la infraestructura de TI y soluciones de Información.

Las empresas contratistas que presten sus servicios a Ecopetrol S.A. deben asegurar que el software instalado en los equipos de cómputo de sus colaboradores se encuentre debidamente licenciado. Esto se refiere mas no se limita a: sistema operativo, herramientas ofimáticas, herramientas contra código malicioso, herramientas de gestión de proyectos en caso de requerirse, herramientas de manejo de planos, herramientas de compresión, herramientas de lectura de documentos en pdf u otros formatos.

En caso de presentarse algún tipo de reclamación por software ilegal, ésta recaerá sobre el funcionario o empresa contratista responsable en donde se encontrase instalado dicho software; debido a que está atentando contra los derechos de autor.

Por consiguiente, el usuario del software sea funcionario o contratista, debe abstenerse de:
1. Copiar, vender, regalar, distribuir o enajenar el software sin permiso del autor.
2. Estimular, permitir, obligar o presionar a los empleados o contratistas a crear o utilizar copias no autorizadas.
3. Prestar los programas para que sean copiados.
4. Ejecutar un programa en dos o más computadores simultáneamente, a no ser, que esté específicamente permitido en la licencia.
5. Utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como "hacking", software para violentar mecanismos de licenciamiento de aplicaciones, entre otros) sin la debida autorización de la Coordinación de Seguridad Informática (CDN).
6. Utilizar aplicaciones que no sean debidamente autorizadas.
7. Utilizar software o servicios de red que permitan el intercambio de Información sin el debido aval y autorización.
8. Utilizar software que permitan el control remoto sobre cualquier tipo de equipo conectado en la red de datos.
9. Utilizar software que permitan el establecimiento de túneles tipo SSH o proxis.
10. Usar software o hardware que permita vulnerar o evadir los controles establecidos por Ecopetrol S.A.

11. Por otro lado, el usuario de software sea funcionario o contratista, debe aplicar las siguientes medidas preventivas para disminuir los riesgos de contagio de virus informáticos u otro tipo de código malicioso:

- Abstenerse de usar software ilegal.
- Mantener activa y actualizada la última versión del software contra código malicioso en su equipo de cómputo y efectuar escaneos periódicos en búsqueda de software malicioso.
- Utilizar el software de detección de código malicioso antes de leer un dispositivo de almacenamiento externo y antes de utilizar un nuevo software.
- En caso de requerir pruebas de software, hacerlas de manera aislada a la red (software en demostración o pruebas entre otros).

3.3.h 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, 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.i Seguridad de Información en Servicios de Computación en la nube

ECOPETROL con el objetivo de mantener la seguridad de sus activos de información con servicios y procesos en la nube, garantizando la disponibilidad, privacidad, confidencialidad e integridad de estos, aplica las siguientes actividades que mitigan el nivel de riesgo a Ciberincidentes en este entorno:

- Desarrollar ejercicios de análisis de riesgos y establecimiento de prácticas de Seguridad desde las fases iniciales de incorporación a la Nube y durante el ciclo de vida del servicio en la Nube.
- Solicitar las mejores prácticas de protección emitidas por los fabricantes de productos y/o Proveedores de Servicios.
- Solicitar informes SOC 2 o SOC 1 e ISO 27001.
- Vincular en la protección de información y aplicación de Seguridad en la Nube a todas las instancias involucradas: Funcional, Dueños de Procesos, Usuarios, Técnicos, Equipos de Proyectos, Operaciones de TI, Abastecimiento y Jurídica.
- Aplicar las guías y Estándares que defina Ecopetrol para la Seguridad en la Nube.

- Localización y acceso de la información en la nube: Ecopetrol debe tener clara la ubicación de sus datos e información, comprendiendo la regulación, los efectos contractuales y jurídicos tanto de la localización lógica como física; Una vez conociendo dónde residen los datos y cómo se mueven, es importante saber quién está accediendo a ellos y cómo.
- Definir e implementar plan de contingencia para preservar la información de los servicios en la nube.
- Mantener inventario de los servicios en la nube autorizados dentro de las redes corporativas.
- Asegurar que todo tipo de servicio en la nube se diseñe, implemente y opere conforme a las políticas de seguridad y gestión de riesgos del negocio.

3.4 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

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

Documento Nuevo		
Versión	**Fecha dd/mm/aaaa**	**Cambios**
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

Para mayor información dirigirse a:
Elaboró: Erica Reina Ceballos – Daliris Maldonado Gomez Teléfono: 2344000 Buzón: erica.reina@ecopetrol.com.co – daliris.maldonado@ecopetrol.com.co Dependencia: Gerencia de Ciberseguridad y Ciberdefensa

Revisado electrónicamente por:	**Aprobado electrónicamente por:**
ALBERTO LEON LOZANO Profesional Senior Ciberseguridad **Cédula de Ciudadanía No. 79.298.662** Vicepresidencia Digital	**EDGARDO ALFONSO ARRIETA ARTETA** Gerente Ciberseguridad y Ciberdefensa **Cédula de Ciudadanía No. 77.195.540** Vicepresidencia Digital
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.*	