	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 1 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

## I. OBJETIVO

Establecer los lineamientos específicos para identificar, evaluar y dar respuesta a los riesgos de Seguridad de la Información, complementarios a lo señalado en el *Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos*.

## II. BASE NORMATIVA

- Ley N° 30096 – Ley de Delitos Informáticos.
- Ley N° 27806, “Ley de Transparencia y Acceso a la Información Pública”.
- Ley N° 29733, “Ley de Protección de Datos Personales”.
- Ley N° 27785, “Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República”.
- D.L. N° 604 “Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática”.
- D.L. N° 861, “Ley del Mercado de Valores”.
- Decreto Supremo N° 106-2017-PCM, que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN).
- Resolución Ministerial N° 004-2016-PCM del 08.01.2016, donde se aprueba el uso obligatorio de la Norma técnica peruana NTP-ISO/IEC 27001:2014.
- Resolución Ministerial N° 166-2017-PCM del 20.06.2017, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
- Política Corporativa de Seguridad de la Información de PETROPERÚ.
- Reglamento de Seguridad de la Información.
- Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.
- Lineamiento del Sistema de Integridad.

## III. ALCANCE Y RESPONSABILIDAD

La presente normativa es aplicable a todas las dependencias de PETROPERÚ en el desarrollo de la gestión de los distintos riesgos identificados que puedan afectar la Confidencialidad, Integridad y Disponibilidad de la Información de los distintos procesos Nivel 1 de la Empresa.

**Responsabilidades:** La responsabilidad de la identificación, evaluación, respuesta a los Riesgos de Seguridad de la Información, incluyendo la determinación e implementación de sus Planes de Acción para afrontar los Riesgos, corresponde a todo el personal de la Empresa, de acuerdo con su competencia.

La identificación, evaluación y respuesta a los Riesgos, así como la determinación e implementación de Planes de Acción para afrontarlos, debe ser, interactiva e integrada a las actividades de cada dependencia, las cuales deben estar alineadas con los objetivos organizacionales de la Empresa.

**Responsable o Dueño del Proceso:** es la persona o dependencia que realiza las actividades principales del proceso. Responsable de liderar la gestión del proceso y su mejora continua (LA1-ADM-004 – Metodología para la Identificación de Procesos).

- Conformar el equipo de trabajo, que se encargará de identificar, evaluar y establecer la respuesta a los Riesgos de Seguridad de la Información.
- Participar en la identificación de activos de la información.
- Promover la participación del personal y asignación de recursos en la identificación, evaluación y tratamiento de Riesgos de Seguridad de la Información.

Revisión 1

Revisión 2

Revisión 3


Aprobado

ESTE DOCUMENTO HA SIDO REVISADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 2 de 24

**Propietario de los Activos de Información:** Persona o entidad que tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo (*Norma ISO/IEC 27000:2014*).

- Participar en la identificación de activos de la información.
- Mantener actualizado el inventario de activos de la información que se encuentra bajo su responsabilidad.
- Participar en la identificación, evaluación y tratamiento de Riesgos de Seguridad de la Información.

**Oficial de Seguridad de la Información:** Persona, designada por el Titular de la Entidad, responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad (*R.M. 166-2017-PCM*).

- Monitorear el avance de las evaluaciones de riesgos de Seguridad de la Información en los activos de los Procesos y la implementación de los planes de acción establecidos para mitigar estos riesgos.

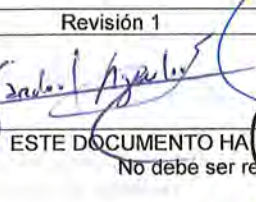

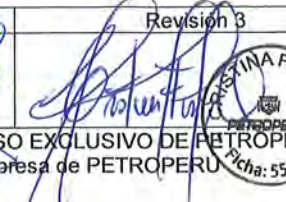
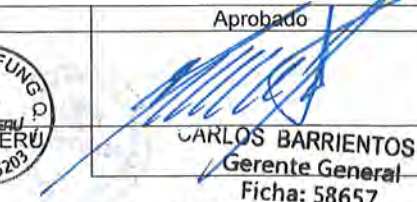
**Analista Control Interno y Seguridad de la Información:** Analista de la Unidad Sistema Control Interno y Seguridad de la Información, cuya misión es planificar, supervisar y evaluar la implementación y administración del Sistema de Gestión de Seguridad de la Información.

- En coordinación con el dueño del Proceso, convocar al Equipo de Trabajo.
- Capacitar en la identificación, análisis y evaluación de riesgos de seguridad de la información al Equipo de Trabajo.
- Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Liderar las reuniones a desarrollarse para el tratamiento de riesgos de seguridad de la información.
- Revisar y presentar a los dueños de los Procesos y al Comité de Seguridad de la Información los resultados de la evaluación y tratamiento de riesgos de Seguridad de la Información.
- Monitorear la implementación del Plan de tratamiento a los Riesgos.

**Equipo de Trabajo:** Equipo multidisciplinario integrado por personal de las diferentes dependencias de la Empresa según corresponda: Dueño del Proceso y Propietario de los Activos de Información, personal con experiencia y/o amplio conocimiento del Proceso y de los Activos de Información que se analizan; así como personal con capacidad de cuestionar y formular críticas constructivas (quienes serán convocados de manera oportuna para integrar el equipo de trabajo para elaborar las matrices de riesgos), bajo la asesoría metodológica de la Sub Gerencia Control Interno y Gestión de Riesgos a fin de efectuar la identificación, evaluación y determinación de la respuesta a los riesgos de Seguridad de la Información, incluyendo la determinación de planes de acción para afrontarlos, mediante la ejecución de talleres de trabajo.


- Desarrollar talleres de trabajo para efectuar la identificación, análisis, evaluación y respuesta a los riesgos de Seguridad de la Información, de cada uno de los diferentes Procesos Nivel 1 de la Empresa.
- Proponer Controles de Seguridad de la Información para los Activos de Información.
- El Equipo de Trabajo debe ser dirigido, por un facilitador Interno (de la Sub Gerencia Control Interno y Gestión de Riesgos) o Externo, para la aplicación de la Metodología y que fomente la participación de todo el Equipo.



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
<p>ESTE DOCUMENTO HA SIDO APROBADO PARA USO EXCLUSIVO DE PETROPERÚ</p> <p>No debe ser reproducido sin autorización expresa de PETROPERÚ</p>			

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 3 de 24

#### IV. DEFINICIONES

En adición a las definiciones de la *Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos LINA1-050*, se añaden las siguientes definiciones, de acuerdo con la Norma ISO/IEC 27000:2014:

**Activo de Información:** Información, otros activos asociados con información e instalaciones de procesamiento de información.

**Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

**Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados.

**Control:** Medida que modifica un riesgo.

Nota 1: Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

Nota 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

**Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada (Persona, Proceso, Sistema u otros Interesados).

**Evaluación del Riesgo:** Proceso para valorar y determinar la gravedad del riesgo.

Nota 1: La evaluación de riesgos ayuda a la decisión sobre el tratamiento del riesgo.

**Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

**Gravedad del Riesgo:** Magnitud de un riesgo, expresados en términos de la combinación de su impacto y de su probabilidad de ocurrencia.

**Identificación del Riesgo:** Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.

**Integridad:** Propiedad de exactitud y lo completo.

**Propietario del Activo de la Información:** Persona o entidad que tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

**Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza dada explote (o se aproveche de) vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a PETROPERÚ.

**Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucradas.

**Vulnerabilidad:** Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

#### V. DESARROLLO DEL LINEAMIENTO

##### A. INVENTARIO DE ACTIVOS DE INFORMACIÓN

La identificación e inventario de activos de información se realiza sobre el proceso asignado y a través de la ejecución de talleres de trabajo, con la participación de los Dueños de los Procesos, Propietarios de los Activos de Información y personal interesado con amplio conocimiento del Proceso. Asimismo, está dirigido por un facilitador Interno (de la Sub Gerencia Control Interno y Gestión de Riesgos) o Externo.

El alcance de la identificación comprende: la información, activos asociados a la información e instalaciones de procesamiento de información; relacionados al proceso en análisis.

CARMEN BELTRÁN VARGAS  
GOLG  
Fecha: 38174

Néstor M. Tello Villegas  
Ficha: 99858  
PETROPERU S.A.


EFIGENIO SANDOVAL AGUIRRE  
Ficha: 33502

ALDA CALDERÓN ANTONIO  
Ficha: 55203

CRISTINA RUIZ  
Ficha: 55203

Revisión 1	Revisión 2	Revisión 3	Aprobado
			
<p>ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ No debe ser reproducido sin autorización expresa de PETROPERÚ</p>			
			<p>CARLOS BARRIENTOS G. Gerente General Ficha: 58657 03 FEB. 2020</p>



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 4 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

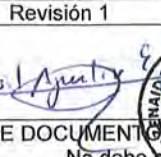
Para el inventario de activos de información se utiliza el Formato del *Anexo 1: Inventario de Activos de Información*, especificando los siguientes datos:

- **Código del Activo:** Se refiere al código de identificación que se asignará al activo de información identificado.
- **Nombre del Activo:** Se refiere al registro del nombre del activo de información.
- **Descripción del Activo:** Se refiere a la descripción breve del contenido del activo de información.
- **Propietario del Activo:** Se refiere al registro del nombre de la persona o dependencia que tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona tenga algún derecho de propiedad sobre el activo.
- **Tipo y Categoría del Activo:** Se referencia de acuerdo con el *Anexo 2: Lista General de Activos de Información*, donde se detalla el tipo y la categoría del activo al que pertenece. *Nota:* Considerar que si se identifica un activo cuyo tipo o categoría no se encuentra registrado en el *Anexo 2*, se debe proceder a incorporarlo en el Formato Inventario de Activos de Información del *Anexo 1: Inventario de Activos de Información*, para su posterior registro y actualización en el *Anexo 2: Lista General de Activos de Información*.
- **Clasificación de la Información (En Pública o Confidencial)**

La clasificación de los activos de información (no incluye otros activos relacionados a información e instalaciones de procesamiento de información) debe alinearse a la clasificación de la información que posee PETROPERÚ, la cual se presume sea Pública, salvo lo siguiente:

- Excepciones al ejercicio del derecho de acceso a la información pública. Información catalogada como Secreta, Reservada y Confidencial, según los artículos 15°, 16° y 17° del Texto Único Ordenado de la Ley N° 27806, "Ley de Transparencia y Acceso a la Información Pública" aprobado por Decreto Supremo N° 043-2003-PCM:
  - La información que contenga consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, salvo que dicha información sea pública. Una vez tomada la decisión, esta excepción cesa si la entidad de la Administración Pública opta por hacer referencia en forma expresa a esos consejos, recomendaciones u opiniones
  - La información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil que están regulados, unos por el inciso 5 del artículo 2 de la Constitución, y los demás por la legislación pertinente.
  - La información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública, en cuyo caso la exclusión del acceso termina cuando la resolución que pone fin al procedimiento queda consentida o cuando transcurren más de seis (6) meses desde que se inició el procedimiento administrativo sancionador, sin que se haya dictado resolución final.
  - La información preparada u obtenida por asesores jurídicos o abogados de las entidades de la Administración Pública cuya publicidad pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial, o de cualquier tipo de información protegida por el secreto profesional que debe guardar el abogado respecto de su asesorado. Esta excepción termina al concluir el proceso.
  - La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso,



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
ESTE DOCUMENTO HA SIDO REPARADO PARA USO EXCLUSIVO DE PETROPERÚ	No debe ser reproducido sin autorización expresa de PETROPERÚ		

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 5 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Estado. En concordancia con la Ley N° 29733, "Ley de Protección de Datos Personales" y su Reglamento, Decreto Supremo N° 003-2013-JUS.

Aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución o por una Ley aprobada por el Congreso de la República.

- En concordancia con el Principio de Reserva de la Ley N° 27785, "Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República" (Artículo 9°), la información que, durante la ejecución de un control, al ser revelada, pueda causar daño a la entidad, a su personal o al Sistema, o dificulte la tarea de este último. Culminado el servicio de control y luego de notificado el informe, el mismo adquiere naturaleza pública y debe ser publicado en su integridad en la página web de la Contraloría General de la República.
- Información Privilegiada o Reservada en concordancia con el D.L. N° 861, "Ley del Mercado de Valores", (Título II, Capítulo III - Información Privilegiada y Deber de Reserva).
- En concordancia con el Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN) - Decreto Supremo N° 106-2017-PCM, la Información de las Instalaciones de la Empresa que forman parte de los recursos, infraestructuras y sistemas esenciales e imprescindibles para mantener y desarrollar las Capacidades Nacionales registrados en el Inventario Nacional como Activos Críticos Nacionales; como son la Refinería Talara, Planta de Ventas Talara y el Oleoducto Nor Peruano, cuya seguridad se gestiona garantizando su intangibilidad o continuidad de sus operaciones.

#### • Tasación de Activos

Se refiere a la adecuada "Valoración del Activo de Información", apoyándose en la evaluación de la afectación o pérdida de los criterios de Confidencialidad (C), Integridad (I) y Disponibilidad (D), bajo el análisis de riesgo inherente (es decir, sin controles existentes); de acuerdo con la escala que se indica para cada criterio:

#### Escala de Valoración del Impacto en la Confidencialidad (C) de la Información

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA O IMPACTO
3	Alta	Es la información clasificada internamente como Confidencial que solo debe ser de conocimiento de las personas autorizadas, debidamente identificadas.	La divulgación no autorizada produce: - Pérdida de la ventaja competitiva. - Uso malicioso en contra de PETROPERÚ. - Pérdidas financieras que no pueden ser absorbidas por PETROPERÚ. - Demandas legales que dañan la imagen y confianza pública de PETROPERÚ.
2	Media	Es la información clasificada internamente como Pública que podrá ser divulgada con Autorización de los propietarios de la misma.	La divulgación no autorizada produce: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por PETROPERÚ.
1	Baja	Es la información divulgada al público general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para PETROPERÚ.




Revisión 1	Revisión 2	Revisión 3	Aprobado
			

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 6 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

### Escala de Valoración del Impacto en la Integridad (I) de la Información

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA O IMPACTO
3	Alta	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: <ul style="list-style-type: none"> <li>- Pérdidas económicas (pérdida, incumplimiento de metas).</li> <li>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable).</li> <li>- Daño de la imagen de PETROPERÚ (daño a nivel nacional e internacional que no se puede reparar en el corto plazo).</li> <li>- Pérdida de la confianza de los usuarios.</li> </ul>
2	Media	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: <ul style="list-style-type: none"> <li>- Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala).</li> <li>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo que está en el límite superior de lo estimado como manejable).</li> <li>- Daño de la imagen de PETROPERÚ (daño a nivel nacional, se puede reparar en el corto plazo).</li> </ul>
1	Baja	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: <ul style="list-style-type: none"> <li>- Pérdidas económicas (no impacta las ganancias, se cumplen las metas).</li> <li>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo, pero este es manejable).</li> <li>- Daño de la imagen de PETROPERÚ (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente).</li> </ul>

### Escala de Valoración del Impacto en la Disponibilidad (D) de la Información


VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA O IMPACTO
3	Alta	Es información o activo indispensable para la continuidad de PETROPERÚ. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: <ul style="list-style-type: none"> <li>- Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio.</li> </ul>

Revisión 1	Revisión 2	Revisión 3	Aprobado
 	 	 	 

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ		CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		LINEAMIENTO Versión: v. 0
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos		Página: 7 de 24

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA O IMPACTO
			<ul style="list-style-type: none"> <li>- Perjuicios legales que afectan la imagen de PETROPERÚ.</li> <li>- Perjuicios económicos que no pueden ser absorbidos por PETROPERÚ.</li> <li>- Problemas sindicales, de gran magnitud.</li> </ul>
2	Media	<p>La disponibilidad de la información es necesaria para la continuidad de PETROPERÚ, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable.</p> <p>El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.</p>	<p>La falta de disponibilidad produce:</p> <ul style="list-style-type: none"> <li>- Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo.</li> <li>- Perjuicios legales que no comprometen la imagen de PETROPERÚ.</li> <li>- Perjuicios económicos que pueden ser absorbidos por PETROPERÚ.</li> </ul>
1	Baja	<p>Es información o activos de apoyo o secundarios para PETROPERÚ.</p> <p>La información se encuentra duplicada en varias fuentes.</p> <p>Si no está disponible no comprometerá procesos operativos importantes.</p>	<p>La falta de disponibilidad produce:</p> <ul style="list-style-type: none"> <li>- Que los niveles de servicio acordados para los procesos operativos importantes, no se vean afectados.</li> <li>- Problemas administrativos y operativos no significativos.</li> <li>- Perjuicios económicos que no son significativos.</li> </ul>

#### ○ Valoración del Activo

La valoración del activo de información identificado, se refiere al máximo valor obtenido de cualquiera de los criterios tasados de Confidencialidad (C), Integridad (I) y Disponibilidad (D), que corresponde a la siguiente escala:

- **Alto:** Activo importante para PETROPERÚ. Su disponibilidad es necesaria para el desarrollo del Proceso.
- **Medio:** Constituye un soporte para los activos importantes de PETROPERÚ. La información puede estar replicada en varias fuentes o existen medios alternos. No compromete el desarrollo del proceso.
- **Bajo:** Activos secundarios, que constituyen información para la toma de decisiones de un Dependencia específica. No compromete el desarrollo del proceso.

Por ejemplo, se identifica al activo de información "Política Comercial y de Descuentos" con los siguientes niveles:

- **Confidencialidad:** Alto (3)
- **Integridad:** Medio (2)
- **Disponibilidad:** Bajo (1)
- **Valoración del Activo:** Se tiene que el criterio de Confidencialidad es Alto (3), el de Integridad es Medio (2) y el de Disponibilidad es Bajo (1); el máximo valor obtenido de los criterios es el de Confidencialidad; por lo tanto, la valoración para este activo es Alto (3).



Revisión 1

Revisión 2

Revisión 3

Aprobado

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

CARLOS BARRIENTOS G.  
Gerente General  
FICHA: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 8 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

## B. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

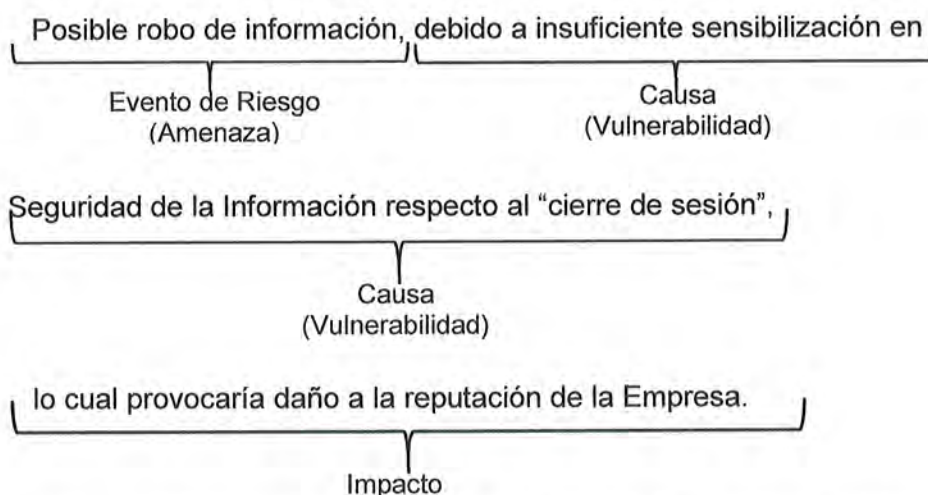
Se inicia con los activos de información cuya valoración resultó con calificación "Alto"; en caso no los haya, se prosigue con los activos cuya valoración resultó con calificación "Medio"; finalmente, si no hay activos cuya valoración resultó con calificación "Alto" y/o "Medio", se prosigue con los activos cuya valoración resultó con calificación "Bajo". Para ello, se utiliza el Anexo 3: *Matriz de Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información*. En esta matriz se debe registrar:

- **Nombre del Activo**, corresponde al activo de información cuya valoración es "Alto" y pasó a esta etapa de identificación de amenazas y vulnerabilidades.
- **Amenazas**, corresponde a un potencial incidente no deseado, que puede resultar en daño a un sistema u organización. Para su identificación se utiliza el Anexo 4: Tabla de Amenazas.
- **Vulnerabilidades**, corresponde a las debilidades de un activo de información o de un control, que puede ser explotada o aprovechada por una o más amenazas. Para su identificación se utiliza el Anexo 5: Tabla de Vulnerabilidades.

## C. IDENTIFICACIÓN DE EVENTOS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

La identificación y descripción de los Eventos de Riesgo de Seguridad de la Información se especifica en base a las Amenazas, Vulnerabilidades y el impacto que producirían, se recomienda describirlo con precisión, según el siguiente ejemplo:

- **Amenaza:** Robo de Información.
- **Vulnerabilidad:** Insuficiente sensibilización en Seguridad de la Información sobre el "cierre de sesión".
- **Impacto:** Daño a la reputación de la Empresa.



A continuación, se debe registrar por separado el Evento de Riesgo, la Causa y el Impacto en las columnas correspondientes de la *Matriz de identificación, evaluación, respuesta a los Riesgos y Planes de Acción* del Anexo 1 del Lineamiento LINA1-050 *Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos*, para facilitar su posterior evaluación.


De igual manera, se registra el "Tipo de Riesgo", según la clasificación de los Riesgos, señalada en el numeral 3 del citado Lineamiento.



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ No debe ser reproducido sin autorización expresa de PETROPERÚ			CARLOS BARRIENTOS G. Gerente General Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 9 de 24

#### D. IDENTIFICACIÓN DE LAS ACTIVIDADES DE CONTROL EXISTENTES

Para la identificación de las actividades de control que existen actualmente en la Empresa para mitigar o reducir los riesgos inherentes, se debe considerar los atributos señalados en el numeral 4: *Identificación de las Actividades de Control Existentes* del Lineamiento LINA1-050 Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.

#### E. EVALUACIÓN DE RIESGOS

La valoración de la Probabilidad y el Impacto, así como, la determinación de la Gravedad, tanto para el Riesgo Inherente (RI), como para el Riesgo Residual (RR), se desarrollará según lo señalado en el numeral 5: *Evaluación de Riesgos* del Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.

Para la evaluación del impacto de los riesgos de Seguridad de la Información, sólo se utilizará como referencia el Anexo 6: *Criterios para evaluar el impacto de los Riesgos de Seguridad de la Información, del presente Lineamiento.*

#### F. RESPUESTA AL RIESGO

Para establecer el tipo de respuesta que se dará a cada riesgo, se tomará como referencia lo señalado en el numeral 6 del Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.

#### G. MATRICES DE PLANES DE ACCIÓN

La definición de los planes de acción se realiza utilizando el Anexo 1: *Matriz de identificación, evaluación, respuesta a los Riesgos y Planes de Acción* del Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.

#### H. DECLARACIÓN DE APLICABILIDAD

Se debe elaborar la Declaración de Aplicabilidad (SoA, Statement of Applicability, por sus siglas en inglés), que contenga el listado de los controles necesarios para implementar el tipo de respuesta elegida (opción de tratamiento); así como la justificación de la inclusión de controles no contemplados en el Anexo A de la norma NTP-ISO/IEC 27001:2014 y la justificación de las exclusiones de controles del mencionado Anexo A. Para ello, se usa el Formato del Anexo 7: *Declaración de Aplicabilidad*, que debe ser generado por la Sub Gerencia Control Interno y Gestión de Riesgos y aprobado por el Comité de Seguridad de la Información.

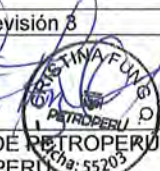
La Declaración de Aplicabilidad se elabora con frecuencia anual, tomando como base las Matrices de Riesgos de Seguridad de la Información de los procesos de la Empresa, que se hayan elaborado en el transcurso del año.

#### I. INFORMACIÓN Y COMUNICACIÓN DE LOS RIESGOS

Será realizada según lo señalado en el numeral 8 del Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos, considerando que las actividades a realizar por el Comité de Control Interno y Gestión de Riesgos, las realizará en este caso el Comité de Seguridad de la Información.

#### J. MONITOREO Y SEGUIMIENTO

Las Matrices aprobadas deben ser enviadas para su consolidación y monitoreo a la Gerencia Corporativa Planeamiento, Gestión y Riesgos.



CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657  
03 FEB. 2020

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Página: 10 de 24

Copia de estos documentos, deben ser comunicados a las Gerencias dueñas o responsables de los procesos según corresponda; las mismas que deben hacer el seguimiento necesario asegurando la implementación de las Actividades de Control establecidas en los Planes de Acción, sin perjuicio del monitoreo de la Sub Gerencia Control Interno y Gestión de Riesgos. Copia de la Matriz de Planes de Acción (Controles) se comunica a las dependencias responsables de la implementación de las actividades de control, las mismas que reportarán con frecuencia trimestral el porcentaje de avance, usando el *Anexo 2: Matriz de Seguimiento al cumplimiento de Planes de Acción para afrontar Riesgos Corporativos del Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.*

## VI. RECOMENDACIONES O PRECISIONES

- En el Anexo 4 "Tabla de Amenazas" y Anexo 5 "Tabla de Vulnerabilidades", se muestra un listado de Amenazas y Vulnerabilidades, lo cual debe ser considerado a título enunciativo y no limitativo.
- Próxima Revisión. 01.12.2021.
- Responsable: Unidad Sistema de Control Interno y Seguridad de la Información.

## VII. CAMBIOS CON RESPECTO A LA VERSIÓN ANTERIOR

Este documento deja sin efecto al Procedimiento PA1-GGR-701 - Análisis y Evaluación de Riesgos en Seguridad de la Información (versión 3).

- Se ha adecuado el presente documento en línea a lo señalado en el *Lineamiento LINA1-050: Metodología para identificar, evaluar y dar respuesta a los Riesgos Corporativos.*
- Se ha modificado la Base Normativa: incluyendo la Resolución Ministerial N° 004-2016-PCM del 08.01.2016, que aprueba el uso obligatorio de la Norma técnica peruana NTP-ISO/IEC 27001:2014, la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"; y excluyendo la R.M. N° 246-2007-PCM.
- Se ha modificado la escala de valorización de Probabilidad e Impacto, considerando ahora cinco (05) Niveles.
- Actualización de nombres de las Dependencias de acuerdo con la nueva Estructura Organizacional de la Empresa.

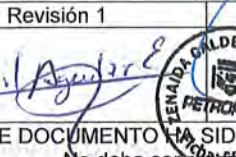
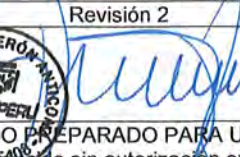

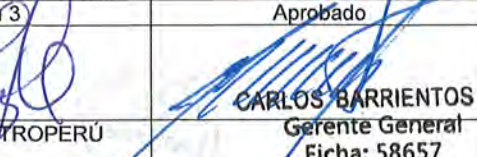
## VIII. PROCESO AL QUE PERTENECE

CÓDIGO	NOMBRE	NIVEL
S6.3	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1

## ANEXOS

- Anexo 1: Inventario de Activos de Información.
- Anexo 2: Lista General de Activos de Información.
- Anexo 3: Matriz de Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información.
- Anexo 4: Tabla de Amenazas.
- Anexo 5: Tabla de Vulnerabilidades.
- Anexo 6: Criterios para evaluar el impacto de los Riesgos de Seguridad de la Información.
- Anexo 7: Declaración de Aplicabilidad.



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ No debe ser reproducido sin autorización expresa de PETROPERÚ			
			CARLOS BARRIENTOS G. Gerente General Ficha: 58657

03 FEB. 2020





**CÓDIGO**  
**LINA1-025**

## PROCEDIMIENTO

Página: 11 de 24

## Anexo 1: Inventario de Activos de Información

Proceso:

**Fecha de aprobación:**

Revisión 2

Revisión 3

Aprobado




Ficha: 55203  
 Gerente Geddy Rios  
 CSTTANA FUNG QUINONES

  
CARLOS BARRIENTOS G.  
Gerente General

03 FEB. 2020      Ficha: 58657



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 12 de 24

## Anexo 2: Lista General de Activos de Información

TIPO	CATEGORIA
Información	Electrónica
	Impresa
	Electrónica e Impresa
Software (Aplicativos)	Software comercial
	Software de terceros
	Software desarrollado internamente
	Otro software
Hardware (Equipos)	Equipo de procesamiento
	Equipo virtual de procesamiento
	Equipo de comunicación
	Otro equipo
Instalaciones	Instalaciones de Procesamiento de Datos
Personas	Responsables de tomar decisiones (Directores, Jefes, entre otros)
	Otros trabajadores
Servicios	Servicios públicos
	Procesamiento y comunicaciones
	Otros servicios



ESTEBAN F. QUINONES  
Gerente Corporativo (e)  
Planeamiento, Gestión y Riesgos  
Fecha: 65203

CARLOS BARRIENTOS G.  
Gerente General  
Fecha: 58657

03 FEB. 2020



Anexo 3: Matriz de Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información

Proceso: \_\_\_\_\_

NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD

Fecha de aprobación: \_\_\_\_\_















Revisión 1

Revisión 2

Revisión 3

Aprobado


ESSE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ  
Ficha: 3354

CRISTINA FLING QUIÑONES  
Gerente Corporativo (e)  
Planeamiento, Gestión y Riesgos  
Ficha: 55203

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 14 de 24

#### Anexo 4: Tabla de Amenazas

AMENAZA	TIPO
Incendio	Daño físico
Daño por agua	
Contaminación	
Destrucción del equipo o los medios	
Polvo, corrosión, congelación	
Fenómeno climático	Eventos naturales
Fenómeno sísmico	
Fenómeno volcánico	
Fenómeno meteorológico	
Inundación	
Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
Pérdida del suministro de electricidad	
Falla del equipo de telecomunicaciones	
Radiación electromagnética	Perturbación debido a radiación
Radiación térmica	
Interceptación de comunicaciones	Compromiso de la información
Robo de medios o documentos	
Robo de equipos	
Hallazgo de medios reciclados o descartados	
Divulgación de información	
Datos de fuentes no confiables	
Adulteración del hardware	
Adulteración del software	
Falla de equipo	Fallas técnicas
Saturación del sistema de información	
Mal funcionamiento del software	
Uso no autorizado del equipo	Acciones no autorizadas
Copia fraudulenta del software	
Uso de software falsificado o copiado	
Procesamiento ilegal de datos	



Revisión 1

Revisión 2

Revisión 3

Aprobado


ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

CRISTINA FONG QUIJONES  
Gerente General  
Planeamiento, Gestión y Riesgos  
Ficha: 55203

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020

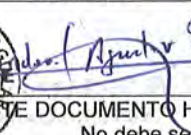

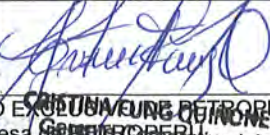



	<b>MANUAL DE PROCEDIMIENTOS DE PETROPERÚ</b>	<b>CÓDIGO LINA1-025</b>
	<b>IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>LINEAMIENTO</b>
	<b>GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos</b>	Versión: v. 0 Página: 15 de 24

AMENAZA	TIPO
Abuso de derechos	<b>Compromiso de funciones</b>
Falsificación de derechos	
Negación de acciones	
Ruptura en la disponibilidad del personal	
Hacking	<b>Hacker, cracker</b>
Ingeniería social	
Acceso no autorizado al sistema	
Bomba/Terrorismo	<b>Terrorismo</b>
Ataque al sistema (ej. DDOS)	
Adulteración del sistema	
Asalto a un empleado	<b>Gente dentro de la Institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)</b>
Chantaje	
Abuso informático	
Robo de información	
Soborno por información	
Ingreso de datos falsificados o corruptos	
Códigos maliciosos (ej. Virus, bomba lógica, troyano).	<b>Otros</b>
Otras amenazas identificadas	


**Nota:** La presente lista de amenazas debe ser considerada a título enunciativo y no limitativo, es decir, pueden presentarse amenazas que serán identificadas por el Equipo de Trabajo.



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
<b>ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ</b> No debe ser reproducido sin autorización expresa de la Gerencia Corporativa Planeamiento, Gestión y Riesgos			
<b>CRISTIANEUNG DE JIMONES</b> Gerente Corporativo (e) Planeamiento, Gestión y Riesgos Ficha: 55203			<b>CARLOS BARRIENTOS G.</b> Gerente General Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Página: 16 de 24

### Anexo 5: Tabla de Vulnerabilidades

VULNERABILIDAD	CATEGORÍA
Mantenimiento insuficiente	Hardware
Falta de esquemas de reemplazo periódicos	
Susceptibilidad a la humedad, al polvo y a la suciedad	
Falta de control eficiente del cambio de configuración	
Susceptibilidad a variación de voltaje	
Susceptibilidad a variaciones de temperatura	
Almacenamiento no protegido	
Falta de cuidado al descartarlo	
Equipo desfasado por vigencia tecnológica	
Pruebas al software inexistentes o insuficientes	Software
Errores conocidos en el software	
No hacer "logout" cuando se sale de la estación de trabajo	
Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
Falta de evidencia de auditoria	
Asignación equivocada de derechos de acceso	
Software ampliamente distribuido	
Interfaz de usuario complicada	
Falta de documentación	
Seteo incorrecto de parámetros	
Fechas incorrectas	
Falta de mecanismos de identificación y autenticación como la autenticación de usuarios	
Tablas de claves no protegidas	
Mala administración de claves	
Habilitación de servicios innecesarios	
Software inmaduro o nuevo	
Especificaciones no claras o incompletas para los desarrolladores	
Falta de control de cambios eficaz	
Descarga y uso incontrolado de software	
Falta de copias de respaldo	
Falta de pruebas de envío o recepción de mensaje	Red



Revisión 1

Revisión 2

Revisión 3

Aprobado


ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de la Gerencia Corporativa

GERENCIA CORPORATIVA  
Gerente Corporativo (a)  
Planeamiento, Gestión y Riesgos  
Ficha: 55203

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0 Página: 17 de 24
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	

VULNERABILIDAD	CATEGORÍA
Líneas de comunicación no protegidas	
Tráfico delicado no protegido	
Mala estructura del cableado	
Falta de identificación y autenticación del destinatario	
Arquitectura de red insegura	
Transferencia de claves en claro	
Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
Conexiones no protegidas de la red pública	
Ausencia del personal	Personal
Procedimientos inadecuados del reclutamiento	
Capacitación de seguridad insuficiente	
Uso incorrecto del software y hardware	
Falta de conciencia de seguridad	
Falta de mecanismos de monitoreo	
Trabajo no supervisado del personal externo o de limpieza	
Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
Ubicaciones en un área susceptible a las inundaciones	
Red inestable de energía eléctrica	
Falta de protección física del edificio, puertas y ventanas	
Falta de un procedimiento formal para el registro y baja de usuarios	Institución
Falta de proceso formal para revisar el derecho de acceso (supervisión)	
Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
Falta de auditorías regulares (supervisión)	
Falta de informes de fallas registradas en los registros del administrador y del operador	
Respuesta inadecuada del mantenimiento del servicio	
Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
Falta de procedimiento de control de cambios	



Revisión 1

Revisión 2

Revisión 3

Aprobado


ESTE DOCUMENTO HA SIDO REPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

CRISTINA FLORES QUIMONES  
Gerente General  
Ficha: 55203

03 FEB. 2020



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Versión: v. 0 Página: 18 de 24

VULNERABILIDAD	CATEGORÍA
Falta de procedimiento formal para el control de la documentación de la institución	
Falta de proceso formal para autorización de información pública disponible	
Falta de asignación apropiada de responsabilidades de seguridad en la información	
Falta de planes de continuidad	
Falta de una política de uso de correos electrónicos	
Falta de procedimientos para introducir software en sistemas operativos	
Faltas de registro en los historiales del administrador y del operador	
Falta de procedimientos para manejo de la información clasificada	
Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
Falta de política formal sobre el uso de computadoras portátiles	
Falta de control de activos que se encuentran fuera del local	
Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
Falta de autorización al acceso a las instalaciones de procesamiento de la información	
Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
Falta de revisiones regulares de la gestión	
Falta de procedimientos para reportar debilidades en la seguridad	
Otras vulnerabilidades identificadas	Otros

**Nota:** La presente lista de vulnerabilidades debe ser considerada a título enunciativo y no limitativo, es decir, pueden presentarse vulnerabilidades que serán identificadas por el Equipo de Trabajo.



Revisión 1	Revisión 2	Revisión 3	Aprobado
 	 	 	 <b>CARLOS BARRIENTOS-G.</b> Gerente General Ficha: 58657

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ  
Gerente Corporativo (a)  
Planeamiento, Gestión y Riesgos  
Ficha: 55203

03 FEB. 2020



Anexo 6: Criterios para evaluar el impacto de los Riesgos de Seguridad de la Información

CRITERIOS	VALOR DE IMPACTO				
	1	2	3	4	5
	MUY BAJO	BAJO	MODERADO	ALTO	MUY ALTO
A Valor del Activo	BAJO Confidencialidad = 1 e Integridad = 1 y Disponibilidad = 1	MEDIO Confidencialidad = 2 o Integridad = 2 o Disponibilidad = 2	MEDIO Confidencialidad = 2 e Integridad = 2 y Disponibilidad = 2	ALTO Confidencialidad = 3 o Integridad = 3 o Disponibilidad = 3	ALTO Confidencialidad = 3 e Integridad = 3 y Disponibilidad = 3
B Pérdida del Activo.	Pequeños daños en el activo.	Pérdida parcial, con opción de recuperación.	Pérdida Parcial, sin opción a recuperación.	Pérdida Total, con opción a recuperación.	Pérdida Total, sin opción a recuperación.
C Interrupción del Servicio.	Menor de Medio (1/2) día.	Entre Medio (1/2) día y un (01) día.	De un (01) día a una (01) semana.	De una (01) semana a un (01) mes.	Mayor que un (01) mes.
D Reputación e Imagen.	Baja y poco extendida.	Baja y muy extendida.	Media y poco extendida.	Media y muy extendida.	Alta y muy extendida.
E Disminución del Rendimiento.	Hasta el 5% variación en los indicadores.	5-10% variación en los indicadores.	10-25% variación en los indicadores.	25 – 50 % variación en los indicadores.	> 50 % variación en los indicadores.

Para evaluar el impacto necesariamente se debe utilizar el criterio "Valor del Activo" y uno o más de los demás criterios, según se estime conveniente; y el valor del impacto será el promedio de los criterios considerados. En caso este promedio no sea un número entero se hará el redondeo al número entero inmediato superior o inferior según corresponda.



Revisión 1

*[Signature]*

Revisión 2

*[Signature]*

Revisión 3

*[Signature]*

Aprobado

*[Signature]*

03 FEB. 2020

Gerente General

Carlos Barrientos G.

Ficha: 58657

CRISTINA FUNG QUINONES

Gerente Corporativo (e)


Planeamiento, Gestión y Riesgos

Ficha: 55203

DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ

No debe ser reproducido sin autorización expresa de PETROPERÚ



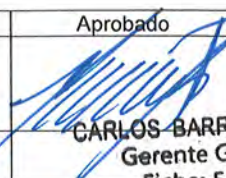
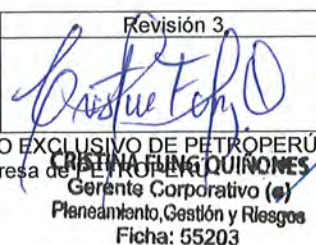
	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ		CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos		Versión: v. 0 Página: 20 de 24

### Anexo 7: Declaración de Aplicabilidad

Fecha: \_\_\_\_\_

Procesos: \_\_\_\_\_

CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN
<b>A.5.</b>	<b>POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>			
	A.5.1 Dirección de Gestión para la Seguridad de Información	A.5.1.1 Políticas de seguridad de información		
		A.5.1.2 Revisión de las políticas de seguridad de información		
<b>A.6.</b>	<b>ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>			
	A.6.1 Organización Interna	A.6.1.1 Funciones de seguridad de información y responsabilidades		
		A.6.1.2 Separación de deberes		
		A.6.1.3 Contacto con autoridades		
		A.6.1.4 Contacto con grupos de interés especial		
		A.6.1.5 Seguridad de información en gerencia de proyectos		
	A.6.2 Dispositivos Móviles y Teletrabajo	A.6.2.1 Política de dispositivo móvil		
		A.6.2.2 Teletrabajo		
<b>A.7.</b>	<b>SEGURIDAD DE RECURSOS HUMANOS</b>			
	A.7.1 Antes del Empleo	A.7.1.1 Evaluación		
		A.7.1.2 Términos y condiciones de empleo		
	A.7.2 Durante el Empleo	A.7.2.1 Responsabilidades de gestión		
		A.7.2.2 Conciencia de seguridad de información, educación y capacitación		
		A.7.2.3 Proceso disciplinario		
	A.7.3 Términos y Cambio de Empleo	A.7.3.1 Término o cambio de las responsabilidades de empleo		
<b>A.8.</b>	<b>GESTIÓN DE ACTIVOS</b>			
	A.8.1 Responsabilidad por Activos	A.8.1.1 Inventario de activos		
		A.8.1.2 Propiedad de activos		
		A.8.1.3 Uso aceptable de activos		
		A.8.1.4 Retorno de activos		
	A.8.2 Clasificación de la Información	A.8.2.1 Clasificación de información		
		A.8.2.2 Etiquetado de información		
		A.8.2.3 Manejo de activos		
	A.8.3 Manejo de Medios	A.8.3.1 Gestión de medios removibles		
		A.8.3.2 Desecho de los medios		
		A.8.3.3 Transferencia de medios físicos		



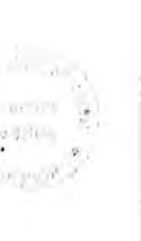
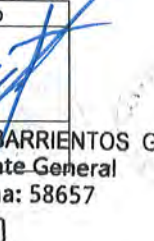
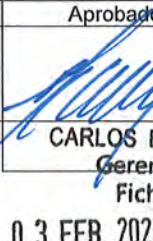
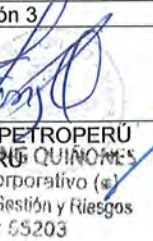
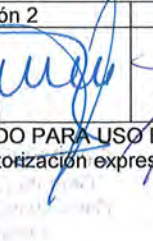
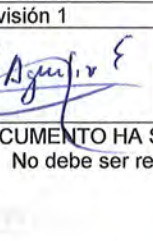
CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

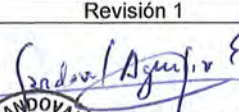
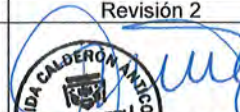
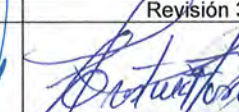
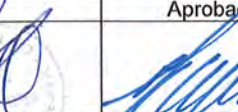
03 FEB. 2020




	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ		CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		LINEAMIENTO
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos		Versión: v. 0 Página: 21 de 24

CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN
<b>A.9.</b>	<b>CONTROL DE ACCESO</b>			
	A.9.1 Requisitos de Negocio para el Control de Acceso	A.9.1.1 Política de control de acceso		
		A.9.1.2 Acceso a redes y servicios de red		
	A.9.2 Gestión de Acceso de Usuario	A.9.2.1 Registro y cancelación de registro de usuarios		
		A.9.2.2 Provisión del acceso de usuario		
		A.9.2.3 Gestión de derechos de acceso privilegiados		
		A.9.2.4 Gestión de la información de autenticación secreta de los usuarios		
		A.9.2.5 Revisión de derechos de acceso de usuarios		
		A.9.2.6 Eliminación o ajuste de derechos de acceso		
	A.9.3 Responsabilidades de Usuarios	A.9.3.1 Uso de información de autenticación secreta		
	A.9.4 Control de Acceso de Aplicación y Sistema	A.9.4.1 Restricción de acceso a la información		
		A.9.4.2 Procedimientos seguros de inicio de sesión		
		A.9.4.3 Sistema de gestión de contraseña		
		A.9.4.4 Uso de programas de utilidad privilegiada		
		A.9.4.5 Control de acceso al código fuente del programa		
<b>A.10.</b>	<b>CRIPTOGRAFÍA</b>			
	A.10.1 Controles Criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos		
		A.10.1.2 Gestión de claves		
<b>A.11.</b>	<b>SEGURIDAD FÍSICA Y AMBIENTAL</b>			
	A.11.1 Áreas de Seguridad	A.11.1.1 Perímetro de seguridad física		
		A.11.1.2 Controles de entrada física		
		A.11.1.3 Seguridad de oficinas, salas e instalaciones		
		A.11.1.4 Protección contra amenazas externas y ambientales		
		A.11.1.5 Trabajo en zonas seguras		
		A.11.1.6 Zonas de entrega y de carga		
	A.11.2 Equipos	A.11.2.1 Situar los equipos y protección		
		A.11.2.2 Servicios públicos de apoyo		
		A.11.2.3 Seguridad del cableado		
		A.11.2.4 Mantenimiento de los equipos		



Revisión 1	Revisión 2	Revisión 3	Aprobado
			
<p>Este documento ha sido preparado para uso exclusivo de PETROPERÚ</p> <p>No debe ser reproducido sin autorización expresa de PETROPERÚ</p> <p>Gerente General</p> <p>Gerente Corporativo (a)</p> <p>Planeamiento, Gestión y Riesgos</p> <p>Ficha: 55203</p>			
<p>CARLOS BARRIENTOS G.</p> <p>Gerente General</p> <p>Ficha: 58657</p> <p>03 FEB. 2020</p>			



	MANUAL DE PROCEDIMIENTOS DE PETROPERÚ	CÓDIGO LINA1-025
	IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	LINEAMIENTO Versión: v. 0
	GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS Sub Gerencia Control Interno y Gestión de Riesgos	Página: 22 de 24


CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN
		A.11.2.5 Retiro de los activos		
		A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones		
		A.11.2.7 Eliminación segura o reúso de equipos		
		A.11.2.8 Equipos de usuarios no atendidos		
		A.11.2.9 Política de escritorio y pantalla limpia		
<b>A.12.</b>	<b>SEGURIDAD DE OPERACIONES</b>			
	A.12.1 Procedimientos Operacionales y Responsabilidades	A.12.1.1 Procedimientos de operación documentados		
		A.12.1.2 Gestión de cambio		
		A.12.1.3 Gestión de capacidad		
		A.12.1.4 Separación de evaluaciones de desarrollo y entornos operacionales		
	A.12.2 Protección contra Malware	A.12.2.1 Control contra malware		
	A.12.3 Copia	A.12.3.1 Copia de información		
	A.12.4 Registro y Monitoreo	A.12.4.1 Registro de eventos		
		A.12.4.2 Protección de información de registro		
		A.12.4.3 Registros de administrador y operador		
		A.12.4.4 Sincronización de reloj		
	A.12.5 Control del Software Operativo	A.12.5.1 Instalación de software en sistemas operacionales		
	A.12.6 Gestión de Vulnerabilidad Técnica	A.12.6.1 Gestión de vulnerabilidades técnicas		
		A.12.6.2 Restricciones en la instalación de software		
	A.12.7 Consideraciones de Auditoría de Sistemas de Información	A.12.7.1 Controles de auditoría de sistemas de información		
<b>A.13.</b>	<b>SEGURIDAD DE COMUNICACIONES</b>			
	A.13.1 Gestión de Seguridad de Redes	A.13.1.1 Controles de redes		
		A.13.1.2 Seguridad de los servicios de redes		
		A.13.1.3 Separación en redes		
	A.13.2 Transferencia de Información	A.13.2.1 Procedimientos y políticas de transferencia de información		
		A.13.2.2 Acuerdos sobre transferencia de información		
		A.13.2.3 Mensajería electrónica		

Revisión 1	Revisión 2	Revisión 3	Aprobado
 	 	 	 





ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa

03 FEB. 2020



	<b>MANUAL DE PROCEDIMIENTOS DE PETROPERÚ</b>		<b>CÓDIGO</b> <b>LINA1-025</b>
	<b>IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>LINEAMIENTO</b>
	<b>GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS</b> Sub Gerencia Control Interno y Gestión de Riesgos		Versión: v. 0 Página: 23 de 24


CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN
		A.13.2.4 Acuerdo de confidencialidad o de no divulgación		
<b>A.14.</b>	<b>ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS</b>			
	A.14.1 Requisitos de Seguridad de los Sistemas de Información	A.14.1.1 Análisis y especificaciones de los requisitos de seguridad de la información A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas A.14.1.3 Protección de las transacciones de servicios de aplicaciones		
	A.14.2 Seguridad en los Procesos de Desarrollo y el Apoyo	A.14.2.1 Política de desarrollo de seguridad A.14.2.2 Procedimientos de control de cambios de sistema A.14.2.3 Revisión técnica de las aplicaciones después de los cambios de la plataforma de operación A.14.2.4 Restricciones a los cambios en los paquetes de software A.14.2.5 Principios de ingeniería de sistemas seguros A.14.2.6 Entorno de desarrollo seguro A.14.2.7 Desarrollo de externalización A.14.2.8 Pruebas de seguridad del sistema A.14.2.9 Pruebas de aceptación del sistema		
	A.14.3 Datos de Pruebas	A.14.3.1 Protección de datos de prueba		
<b>A.15.</b>	<b>RELACIONES DE PROVEEDORES</b>			
	A.15.1 Seguridad de la Información en la Relación con los Proveedores	A.15.1.1 Política de seguridad de información para la relación con los proveedores A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores A.15.1.3 Cadena de suministro de tecnología de información y comunicaciones		
	A.15.2 Gestión de la Prestación de Servicios de Proveedor	A.15.2.1 Monitoreo y revisión de los servicios de proveedores A.15.2.2 Gestión de cambios de los servicios del proveedor		
<b>A.16.</b>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>			
	A.16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras	A.16.1.1 Responsabilidades y procedimientos A.16.1.2 Informe de eventos de seguridad de información A.16.1.3 Informes de debilidades de seguridad de información		

Revisión 1	Revisión 2	Revisión 3	Aprobado
			
Néstor M. Tello Vilca Ficha: 9985 PETROPERU S.A.	CRISTINA FUMIGUIONES Gerente Operativo (*) Planeamiento, Gestión y Riesgos Ficha: 55203		CARLOS BARRIENTOS G. Gerente General Ficha: 58657

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de la Gerencia Operativa (\*)

03 FEB. 2020



	<b>MANUAL DE PROCEDIMIENTOS DE PETROPERÚ</b>		<b>CÓDIGO</b> <b>LINA1-025</b>
	<b>IDENTIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>LINEAMIENTO</b> Versión: v. 0
	<b>GERENCIA CORPORATIVA PLANEAMIENTO, GESTIÓN Y RIESGOS</b> Sub Gerencia Control Interno y Gestión de Riesgos		Página: 24 de 24

CLÁUSULA N°	OBJETIVOS DE CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información		
		A.16.1.5 Respuesta a los incidentes de seguridad de información		
		A.16.1.6 Aprendiendo de los incidentes de seguridad de la información		
		A.16.1.7 Recolección de evidencia		
<b>A.17.</b>	<b>ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</b>			
	A.17.1 Continuidad de Seguridad de Información	A.17.1.1 Planeando la continuidad de seguridad de información		
		A.17.1.2 Implementación de la continuidad de seguridad de información		
		A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información		
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información		
<b>A.18.</b>	<b>CUMPLIMIENTO</b>			
	A.18.1 Cumplimiento de los Requisitos Legales y Contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales		
		A.18.1.2 Derechos de propiedad intelectual		
		A.18.1.3 Protección de registros		
		A.18.1.4 Privacidad y protección de datos personales		
		A.18.1.5 Regulación de controles criptográficos		
	A.18.2 Revisiones de Seguridad de Información	A.18.2.1 Revisión independiente de seguridad de la información		
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad		
		A.18.2.3 Revisión de cumplimiento técnico		



Revisión 1	Revisión 2	Revisión 3	Aprobado
			

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ  
No debe ser reproducido sin autorización expresa de PETROPERÚ  
Gerente General (G)  
Planeamiento, Gestión y Riesgos  
Ficha: 55203

CARLOS BARRIENTOS G.  
Gerente General  
Ficha: 58657

03 FEB. 2020