



<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 1 de 35</b>



# **REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.**


**VIGENTE DESDE EL 19.01.2011**

**APROBADO CON ACUERDO DE DIRECTORIO N°0114-2010-PP  
DE FECHA 28.12.2010**

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 2 de 35</b>

## ÍNDICE

<b>CAPITULO I: DISPOSICIONES GENERALES .....</b>	<b>4</b>
ARTÍCULO 1º: Objetivo .....	4
ARTÍCULO 2º: Propósito .....	4
ARTÍCULO 3º: Ámbito de la Aplicación .....	4
ARTÍCULO 4º: Base Legal y Normatividad Interna .....	4
4.1. Normas Legales .....	4
4.2. Normatividad Interna .....	5
ARTÍCULO 5º: Importancia de la Seguridad de la Información .....	5
ARTÍCULO 6º: Organización y Funciones en Seguridad de la Información.....	6
6.1. Directorio.....	6
6.2. Gerente General.....	6
6.3. Gerentes de Estructura Básica .....	6
6.4. Propietario del Activo de Información .....	7
6.5. Oficinas de Tecnologías de Información y Comunicaciones .....	7
6.6. Usuarios .....	7
6.7. Organización de Seguridad de la Información .....	7
6.8. Comité de Seguridad de la Información .....	8
ARTÍCULO 7º: Inobservancias a la Seguridad de la Información .....	8
<b>CAPÍTULO II: POLÍTICA.....</b>	<b>9</b>
ARTÍCULO 8º: Política Corporativa de Seguridad de la Información.....	9
<b>CAPÍTULO III: RECURSOS HUMANOS, COLABORADORES Y USUARIOS .....</b>	<b>9</b>
ARTÍCULO 9º: Requisitos de Seguridad de la Información en Contratos de Trabajo, Civiles y Comerciales.....	9
<b>CAPÍTULO IV: SEGURIDAD FÍSICA Y DEL ENTORNO .....</b>	<b>11</b>
ARTÍCULO 10º: Seguridad de Equipos Fuera de las Instalaciones de PETROPERU .....	11
ARTÍCULO 11º: Seguridad de los Centros de Cómputo .....	12
<b>CAPÍTULO V: GESTIÓN DE COMUNICACIONES Y OPERACIONES.....</b>	<b>13</b>
ARTÍCULO 12º: Control de Riesgos de Seguridad de la Información de los Servicios de Ofimática.....	13
ARTÍCULO 13º: Intercambio de Software o de Información por Voz, Fax y/o Video.....	14
ARTÍCULO 14º: Transmisión de Información Confidencial, Sensible o Crítica .....	14
ARTÍCULO 15º: Uso de Correo Electrónico y Adjuntos.....	14
ARTÍCULO 16º: Retención y Eliminación de Registros .....	16
<b>CAPÍTULO VI: CONTROL DE ACCESOS .....</b>	<b>17</b>
ARTÍCULO 17º: Control de Accesos .....	17
ARTÍCULO 18º: Protector de Pantalla y Escritorio Limpio.....	17
ARTÍCULO 19º: Uso Servicios de Red.....	18
ARTÍCULO 20º: Informática Móvil.....	19
<b>CAPÍTULO VII: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS .....</b>	<b>20</b>
ARTÍCULO 21º: Adquisición y Desarrollo.....	20
ARTÍCULO 22º: Uso de Controles Criptográficos .....	20

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 3 de 35</b>

## **CAPÍTULO VIII: RECURSOS HUMANOS E INFORMACIÓN CONFIDENCIAL ..... 20**

ARTÍCULO 23º: Protección de Datos y Privacidad de la Información Personal..... 20

## **CAPÍTULO IX: DISPOSICIONES COMPLEMENTARIAS ..... 21**

PRIMERA: Aplicación Supletoria ..... 22

SEGUNDA: Propuesta de Procedimientos, Formatos y Otros..... 22

TERCERA: Aprobación de Procedimientos, Formatos y Otros ..... 22

CUARTA: Vigencia del Reglamento..... 22

QUINTA: Difusión y Supervisión del Reglamento..... 22

## **CAPÍTULO X: ANEXOS ..... 23**

ANEXO 1: Glosario de Términos ..... 23


ANEXO 2: Modelo de Texto de Confidencialidad para Servicio de Correo Electrónico ..... 28

ANEXO 3: Requisitos de Seguridad de la Información con Empleados, Colaboradores, Usuarios y Otros Terceros ..... 29

ANEXO 4: Modelo Cronograma de Retención de Registros ..... 31

ANEXO 5: Transmisión de Información Confidencial, Crítica o Sensible..... 33

ANEXO 6: Composición del Comité de Seguridad de la Información ..... 34

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 4 de 35</b>

## **CAPITULO I: DISPOSICIONES GENERALES**

### **ARTÍCULO 1º: Objetivo**

El Reglamento de Seguridad de la Información, desarrollado con sujeción a la Política Corporativa de Seguridad de la Información y la Norma Técnica Peruana NTP-ISO/IEC 17799:2007, tiene por objetivo:

- Asegurar una apropiada salvaguarda de todos los activos de información a los que PETROPERU sea sensible.
- Proporcionar asesoría para la Seguridad de la Información.
- Permitir una aplicación consistente de los controles de seguridad de la información.
- Acceder a una defensa contra alegatos legales.
- Reducir y controlar los riesgos legales, comerciales y tecnológicos.
- Proteger la buena imagen empresarial de PETROPERÚ.

### **ARTÍCULO 2º: Propósito**

La información y los medios para su generación, tratamiento, transmisión y almacenamiento, son activos importantes de la institución y por ello requieren ser protegidos. La disponibilidad, integridad y confidencialidad de la información, son esenciales para mantener la operatividad, competitividad, efectividad, proactividad, confiabilidad, continuidad e imagen de PETROPERÚ.

Para lograr este fin, es necesario contar con un documento normativo, el cual debe ser redactado de una manera clara y concisa, para comprensión y aplicación de todos los usuarios. Se requiere educar y capacitar en forma clara y detallada, sobre las consecuencias de su inobservancia.


### **ARTÍCULO 3º: Ámbito de la Aplicación**

El presente Reglamento será de aplicación general y obligatoria para Miembros del Directorio, Gerente General, Gerentes de Estructura Básica y Complementaria, Trabajadores en General, Practicantes, Consultores, Prestadores de Servicios Profesionales, Personal de Contratistas y otros, en adelante “usuarios”, que necesiten tener acceso a la información o recursos de tratamiento de la información de PETROPERÚ, mientras desempeñen sus labores en la misma y exista vínculo laboral, civil o comercial y, de acuerdo a convenios o normatividad específica, incluso cuando cese sus funciones.

### **ARTÍCULO 4º: Base Legal y Normatividad Interna**

#### **4.1. Normas Legales**

- Ley N° 27785 Ley Orgánica del Sistema Nacional de Control de la Contraloría General de la República.
- Ley N° 27806 Ley de Transparencia y Acceso a la Información Pública, TUO de fecha 22.04.2003, y su Reglamento DS N° 072-2003-PCM de fecha 06.08.2003.
- Ley N° 28716 Ley de Control Interno de las Entidades del Estado.

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002</b> <b>Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1</b> <b>Página: 5 de 35</b>

- Resolución de Contraloría General N° 320-2006-CG de fecha 11.10.2006. Aprueban las Normas de Control Interno, aplicables a las Entidades del Estado.
- Resolución Ministerial N° 246-2007-PCM de fecha 22.08.2007. Aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007.
- Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 2ª Edición.
- Resolución de Contraloría N° 458-2008-CG de fecha 30.10.2008. Guía para la Implementación de Control Interno en las Entidades del Estado.

#### **4.2. Normatividad Interna**


- Política Corporativa de Seguridad de la Información de PETROPERÚ. Aprobada con Acuerdo de Directorio N° 040-2010 de fecha 29.04.2010.
- Código de Integridad de PETROPERÚ. Aprobado con Acuerdo de Directorio N° 004-2010 de fecha 28.01.2010 y Acuerdo de Directorio N° 019-2009 de fecha 12.03.2010.
- Normas Internas de Conducta de PETROPERÚ, para la Comunicación de Hechos de Importancias, Información Reservada y otras Comunicaciones. Aprobada con Acuerdo de Directorio N° 105-2009 de fecha 30.11.2009.
- Código de Buen Gobierno Corporativo de PETROPERÚ. Aprobado con Acuerdo de Directorio N° 107-2010-PP de fecha 30.11.2010.
- Reglamento Interno del Comité de Buenas Prácticas de Gobierno Corporativo de PETROPERÚ. Aprobado con Acuerdo de Directorio N° 044-2010 de fecha 12.05.2010.
- Reglamento Interno de Trabajo de PETROPERÚ.
- Política de Conflicto de Intereses de PETROPERÚ.
- Reglamento de Organización y Funciones (ROF) de PETROPERÚ. Aprobado con Acuerdo de Directorio N° 061-2009-PP de fecha 14.07.2009.
- Manual de Organización y Funciones (MOF) de PETROPERÚ.

#### **ARTÍCULO 5º: Importancia de la Seguridad de la Información**

La información es cada vez más esencial en los procesos de negocio para conseguir y mantener la rentabilidad y competitividad, gestionar adecuadamente los recursos internos y externos, gestionar eficazmente las operaciones, obtener y mantener clientes y cuota de mercado, así como gestionar y mantener el conocimiento, entre otros.

Las organizaciones y su información enfrentan amenazas y vulnerabilidades crecientes que afectan los elementos de los procesos de negocio, los comúnmente denominados “fallos de seguridad” que pueden ser variados, incluyendo fraudes informáticos, fallo electrónico, espionaje, error humano, sabotaje, vandalismo, incendios, inundaciones u otros. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Dado que la información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación, ésta deberá protegerse

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 6 de 35

adecuadamente, cualquiera que sea la forma que tome o los medios por los que se comparta o almacene en PETROPERU.

Los usuarios deben ser conscientes, que la importancia de la información es proporcional al valor empresarial de sus procesos, lo que hace necesario adoptar mecanismos de gestión de seguridad de la información, entre los que se pueden contar la política, reglamento, procedimientos, estructura organizacional y soluciones tecnológicas sobre la base de estándares probados y reconocidos, tanto a nivel nacional como internacional.

La seguridad de la información se define como la salvaguarda de la información para:

- **Su confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la información;
- **Su integridad**, asegurando que la información y sus métodos de proceso sean exactos y completos;
- **Su disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la información cuando la requieran.

## ARTÍCULO 6º: Organización y Funciones en Seguridad de la Información

La organización y funciones para la seguridad de la información se asignan de la forma siguiente:

### 6.1. Directorio


- Aprobar la Política Corporativa de Seguridad de la Información y sus modificaciones.
- Aprobar el Reglamento de Seguridad de la Información y sus modificaciones.

### 6.2. Gerente General

- Difundir la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información.
- Aprobar los procedimientos y cualquier otra disposición complementaria de seguridad de la información, que las Gerencias de la Estructura Básica propongan según su competencia.
- Aprobar las propuestas del Comité de Seguridad de la Información, para asegurar el correcto entendimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información y, que todos los usuarios se comprometan razonablemente a su cumplimiento.
- Aprobar las iniciativas para mejorar la seguridad de la información.
- Aprobar la evaluación anual y el plan anual de la gestión de seguridad de la información.

### 6.3. Gerentes de Estructura Básica

- Difundir la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información, asegurando su razonable entendimiento y cumplimiento.
- Asignar recursos para el cumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de Información, requeridos por el Comité de Seguridad de la Información.

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 7 de 35</b>

- Proponer a Gerencia General, según su competencia, la aprobación de los procedimientos y cualquier otra disposición complementaria de Seguridad de la Información.

#### **6.4. Propietario del Activo de Información**

- Velar por la seguridad del activo de información que está a su cargo.
- Supervisar la implementación y el mantenimiento de los controles que aplican al activo de información.
- Clasificar la información en términos de su valor, confidencialidad, criticidad y sensibilidad para PETROPERÚ.

#### **6.5. Oficinas de Tecnologías de Información y Comunicaciones**

- Administrar, monitorear y operar en forma segura las redes y sistemas informáticos de PETROPERÚ.
- Facilitar los mecanismos técnicos que permitan dar cumplimiento a la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información.
- Hacer cumplir las normas y procedimientos de Seguridad Informática.


#### **6.6. Usuarios**

- Proponer alternativas de mejoras en la seguridad de la información.
- Reportar cualquier incidente de seguridad de la información a la Organización de Seguridad de la Información o al Comité de Seguridad de la Información, según procedimiento de gestión de incidentes.
- Incluir la cláusula confidencialidad y de seguridad de la información en los contratos con terceros, clientes y proveedores.
- Asumir responsabilidad en la generación, tratamiento, transmisión y almacenamiento de los activos de información que usan en el ejercicio de sus funciones.

#### **6.7. Organización de Seguridad de la Información**

- Proponer al Comité la actualización de la Política Corporativa, el Reglamento y los Procedimientos de seguridad de la información.
- Revisar y proponer propietarios para cada activo de información.
- Formular criterios de clasificación de la información.
- Revisar y mantener actualizado el inventario de activos de información.
- Presentar normas complementarias, prácticas de gestión y procedimientos, diseñados para proporcionar una convicción razonable para que todos los usuarios cumplan la política, reglamento y procedimientos de seguridad de la información.
- Analizar y hacer seguimiento sobre los incidentes en seguridad de la información.
- Coordinar la ejecución periódica de la evaluación de riesgos y proponer controles de tratamiento de riesgos, en línea con el Sistema de Control Interno.
- Asegurar que la implementación de controles de seguridad de la información sea ejecutada.
- Desarrollar y proponer planes y programas de concientización y capacitación en temas de seguridad de la información.



<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 8 de 35</b>

#### **6.8. Comité de Seguridad de la Información**


- Identificar las metas de seguridad de la información, relacionarlas con las exigencias organizacionales e integrarlas en los procesos relevantes.
- Planificar y coordinar la ejecución periódica de la evaluación de riesgos y proponer controles para el tratamiento de los mismos.
- Proponer planes, programas y presupuesto para mantener la concientización de la seguridad de la información.
- Proponer la actualización de la Política Corporativa, Reglamento y Procedimientos de seguridad de la información.
- Proponer a la Gerencia General la inclusión de roles y responsabilidades de seguridad de la información en el Reglamento de Organización y Funciones, Manual de Organización y Funciones y, Descripciones de Puesto.
- Monitorear el cumplimiento de la Política Corporativa, Reglamento y Procedimientos de seguridad de la información, verificando su efectividad y correcta implementación.
- Proponer convenios con especialistas en seguridad de la información para recibir asesoría.
- Solicitar los recursos necesarios para establecer y respaldar las iniciativas, para mejorar la seguridad de la información.
- Reunirse ordinariamente, según su plan anual de trabajo, por lo menos cada dos (2) meses, utilizando la facilidad de videoconferencia con la que cuenta PETROPERÚ, de las cuales dos (2) serán presenciales; y, extraordinariamente cuando sea convocado por Gerencia General o alguno de sus miembros.
- Los miembros designados en el Comité de Seguridad de Información, salvo los representantes de la Gerencia Departamento Tecnologías de Información y Comunicaciones y de la Unidad Seguridad de Oficina Principal, serán renovados cada dos (2) años. La designación es hecha por Gerencia General, conforme a la composición establecida en el Anexo 6.
- Lo no previsto expresamente en el presente Reglamento, será resuelto por el Comité de Seguridad de la Información.

#### **ARTÍCULO 7º: Inobservancias a la Seguridad de la Información**

El no cumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información, así como de cualquier otro proceso, lineamiento o pauta de uso obligatorio, derivados de éstos, puede resultar en una acción disciplinaria para el empleado o penalidad<sup>1</sup> para el contratista por parte de PETROPERÚ, dependiendo del tipo y severidad de la infracción o de la inobservancia.

<sup>1</sup> Además de la separación del colaborador infractor.



		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 9 de 35

## CAPÍTULO II: POLÍTICA

### ARTÍCULO 8º: Política Corporativa de Seguridad de la Información

Petróleos del Perú – PETROPERÚ S.A. es una empresa estatal de derecho privado dedicada al transporte, refinación y comercialización de combustibles y demás derivados de petróleo, y gestiona la seguridad de la información relacionada con sus actividades, productos y servicios en forma responsable, en concordancia con la normatividad vigente y los siguientes lineamientos:


- El establecimiento de un conjunto de actividades que permitan preservar y asegurar la confidencialidad, integridad y disponibilidad de la información, viabilizando la competitividad, rentabilidad, integridad y transparencia de la Empresa.
- La periódica identificación, evaluación, tratamiento y monitoreo de los riesgos de seguridad de la información relevantes a la Empresa.
- La investigación, respuesta oportuna y recuperación efectiva ante incidentes relacionados con la seguridad de la información.
- La comunicación oportuna y permanente de las políticas y procedimientos de la seguridad de la información definidos, asegurando razonablemente que sean comprendidos y se encuentren disponibles para todos los trabajadores y colaboradores de la Empresa.
- La responsabilidad por el uso de la información crítica y sensible por todos los trabajadores y colaboradores de la Empresa.
- El cumplimiento de los requerimientos dispuestos en las disposiciones legales y contractuales aplicables a la Seguridad de la Información, que comprenden a la Empresa.
- El fortalecimiento de los valores, la sensibilización y el compromiso de todos los trabajadores y colaboradores, de velar por el cumplimiento de la presente política.

## CAPÍTULO III: RECURSOS HUMANOS, COLABORADORES Y USUARIOS


### ARTÍCULO 9º: Requisitos de Seguridad de la Información en Contratos de Trabajo, Civiles y Comerciales

**Objetivo:** Controlar y mantener la seguridad, para que los activos y recursos de tratamiento de la información de PETROPERÚ sean accesibles en forma segura por los usuarios. Establecer los requerimientos de confidencialidad que reflejen las necesidades de la organización para la protección de su información.

**Alcance:** Todos los usuarios de PETROPERÚ.

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002</b> <b>Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1</b> <b>Página: 10 de 35</b>

- a. Cuando el negocio requiera del acceso de colaboradores, se deberá realizar una evaluación del riesgo para determinar sus implicancias sobre la seguridad de la información y las medidas de control que requieren. Asimismo PETROPERÚ deberá evaluar y medir periódicamente el nivel de seguridad ofrecido por los servicios de terceros, incorporando métricas para el monitoreo.
- b. Asegurar que los usuarios y colaboradores entiendan su responsabilidad, dentro de las funciones y ámbito para los que han sido contratados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones y sus activos de información.
- c. Los candidatos a ser contratados, empleados o colaboradores, para funciones donde se tendrá acceso a información sensible, crítica o confidencial, deben ser evaluados y seleccionados en forma rigurosa.
- d. La responsabilidad de los empleados con acceso a la información sensible o crítica o confidencial de PETROPERÚ, deberá estar definida en la Descripción de Puesto y reflejarse en el Manual de Organización y Funciones. Los empleados deberán observar las normas y mantener el debido cuidado con la comunicación que fluye al exterior.
- e. El acceso a los recursos de la información o archivos, debe limitarse al empleado contratado, que ha sido autorizado como responsable para la utilización o custodia de los mismos. La responsabilidad, en cuanto a la utilización y custodia, debe evidenciarse a través de registros, inventarios o cualquier otro documento o medio que permita llevar un control efectivo sobre los recursos de la información o archivos.
- f. Los empleados y practicantes de PETROPERÚ y, los colaboradores con sus contratistas, deben firmar un acuerdo de confidencialidad al ser contratados. La función Recursos Humanos es responsable de realizar esta labor con los empleados y, el Administrador del Contrato con los colaboradores.
- g. La función Recursos Humanos, al igual que el Administrador del Contrato, deben informar a las áreas competentes sobre el personal y colaboradores que han culminado su vínculo laboral o relación contractual respectivamente, con el fin de prevenir accesos no autorizados a la información, sistemas, oficinas o equipos de PETROPERÚ.
- h. Los empleados y colaboradores, que desarrollan programas o proyectos para PETROPERÚ, deben firmar acuerdos de derecho de propiedad, reconociendo que dichos programas, patentes, inventos y proyectos son de propiedad integral de PETROPERÚ.
- i. La función Recursos Humanos debe incluir los temas de Seguridad de la Información en las charlas de inducción a todo el personal y practicantes que ingresan a PETROPERÚ; y, deberá considerar dentro del programa anual de

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 11 de 35

capacitación, temas de seguridad de la información que comprenda difusión, evaluación y monitoreo.

- j. Las funciones Recursos Humanos y Legal deben revisar que en los contratos se incluya los acuerdos de confidencialidad y de derecho de la propiedad, cada vez que se produzcan cambios en la modalidad de contratación de los empleados.
- k. Los privilegios asignados a cada empleado deben ser revisados, cuando sean transferidos, cambien de puesto o modalidad de empleo.
- l. Los empleados, cualquiera fuere su tipo de relación laboral, deben comprender y familiarizarse con la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información, el Código de Integridad y el Reglamento Interno de Trabajo de PETROPERÚ.
- m. Todos los empleados, para no contravenir la Política y Normas sobre Conflicto de Intereses y, el Código de Integridad, deben informar a la función Recursos Humanos sobre cualquier circunstancia personal que pueda generar una situación de conflicto entre sus intereses personales y los intereses de PETROPERÚ.


#### CAPÍTULO IV: SEGURIDAD FÍSICA Y DEL ENTORNO

##### ARTÍCULO 10º: Seguridad de Equipos Fuera de las Instalaciones de PETROPERÚ

**Objetivo:** Prevenir pérdidas y daños o comprometer los equipos, así como la interrupción de las actividades de la organización. El equipo deberá estar físicamente protegido de las amenazas. También se deberá considerar su instalación, incluyendo su uso fuera del local, y disponibilidad. Pueden requerirse medidas o controles especiales contra riesgos de accesos no autorizados y la infraestructura necesaria para proteger los sistemas de apoyo.

**Alcance:** Todos los usuarios de PETROPERÚ.

- a. El uso, fuera de las instalaciones de PETROPERÚ, de cualquier equipo portátil que contenga información, se realizará de acuerdo a los niveles de autorización.
- b. Las áreas de Tecnologías de Información y Comunicaciones realizarán periódicamente una revisión de los equipos, evaluarán los riesgos y aplicarán los controles o acciones para preservar la integridad y el contenido de los equipos que salen fuera de las instalaciones de PETROPERÚ.
- c. Los usuarios no deben realizar cambios en los controles de seguridad, ni en las configuraciones de los equipos establecidas por las áreas de Tecnologías de Información y Comunicaciones.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 12 de 35


- d. Los usuarios no deben dejar expuestos al uso y/o disposición de terceros, en lugares de acceso público, los equipos informáticos o de tratamiento de la información, de propiedad de PETROPERÚ.
- e. Todos los equipos de tratamiento de la información, que deban ser usados fuera de las instalaciones de PETROPERÚ, deben contar con clave y una póliza de seguros de reposición.

## ARTÍCULO 11º: Seguridad de los Centros de Cómputo

**Objetivo:** Prevenir y evitar pérdidas, daños o eventos que comprometan las instalaciones, infraestructura, equipos, datos y servicios de los Centros de Cómputo de las Operaciones y del Centro de Cómputo Principal de PETROPERÚ.

**Alcance:** Usuarios y terceros.

- a. Los centros de cómputo de PETROPERÚ deben estar instalados y protegidos en áreas seguras, donde se proporcione un nivel de seguridad contra accesos no autorizados, robo, daño y otros, sobre la base de controles de acceso físico perimetrales.
- b. El Centro de Cómputo Principal de PETROPERÚ debe contar con:
  - i. Un área controlada y restringida sólo a personas autorizadas, y que por sus funciones dentro de ella se le concede la autorización. Los derechos de acceso a esta área, de todos los usuarios permitidos, deben ser revisados cada tres (3) meses.
  - ii. Un sistema de ingreso, a esta área sensible y crítica, controlado en todo momento, con un registro de ingreso obligatorio que debe contener como mínimo la identificación del usuario, fecha y hora de ingreso / salida, manteniendo un rastro de auditoría de los accesos.
  - iii. Un registro de acceso de personas que ingresan por visita o trabajos específicos y que no pertenecen a esta área. El permiso de ingreso será otorgado por el Departamento Tecnologías de Información y Comunicaciones de PETROPERU. Estas personas, antes de ingresar, se deberán registrar en la bitácora de ingreso y en todo momento estarán acompañadas por el Operador de Turno del Centro de Cómputo.
  - iv. Mecanismos de protección física contra daños por fuego, cuyo equipo contra incendios debe resguardar toda el área del Centro de Cómputo Principal.
  - v. Controles de monitoreo de condiciones ambientales. La temperatura y humedad deberán ser monitoreadas por el Operador de Turno y responder oportunamente ante las alertas.
  - vi. Aviso que indique, que está terminantemente prohibido ingerir alimentos y bebidas en el Centro de Cómputo Principal.
  - vii. Aviso que indique, que está terminantemente prohibido encender fuego y fumar en el Centro de Cómputo Principal.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 13 de 35

- viii. Equipos de suministro de energía eléctrica, como UPS y generador eléctrico, que se deben revisar y probar regularmente y en forma inopinada, para asegurar su capacidad y operatividad ante una contingencia eléctrica.
- ix. Un programa de mantenimiento preventivo para todos los equipos.
- c. La Gerencia Departamento Tecnologías de Información y Comunicaciones deberá establecer los mecanismos de control de activos y recursos informáticos, así como las medidas de seguridad física para el acceso restringido a todos los Centros de Cómputo de PETROPERÚ.
- d. La seguridad física de los Centros de Cómputo de PETROPERÚ, estará a cargo del área responsable de la seguridad de instalaciones de Oficina Principal y las Operaciones.
- e. Los acápites del literal b), en lo que corresponda, serán de aplicación para los Centros de Cómputo y Salas de Telecomunicaciones de las Operaciones.


## CAPÍTULO V: GESTIÓN DE COMUNICACIONES Y OPERACIONES

### ARTÍCULO 12º: Control de Riesgos de Seguridad de la Información de los Servicios de Ofimática

**Objetivo:** Controlar los riesgos del negocio asociados con los sistemas de ofimática que proporcionan facilidades para difundir más rápidamente y para compartir la información del negocio usando una combinación de documentos, estaciones de trabajo y comunicaciones móviles, correos escrito y de voz, comunicaciones de voz en general, multimedia, servicios y recursos postales y máquinas de fax, entre otros.

**Alcance:** Todos los usuarios de PETROPERÚ.

- a. Es responsabilidad de cada usuario, recoger los documentos enviados a imprimir en las impresoras de PETROPERÚ de manera inmediata.
- b. Es responsabilidad de cada área, destruir los documentos impresos que ya no sirven y que contienen información confidencial, crítica o sensible.
- c. Los usuarios deben ubicar los sistemas y dispositivos de ofimática a su cargo, impresoras, fax y fotocopadoras, en ambientes controlados para evitar que la información sea interceptada por personal o colaboradores no autorizados, o por personas externas de PETROPERÚ.
- d. Los usuarios no deben enviar información confidencial para ser impresa en una impresora de red, sin que haya una persona autorizada que proteja su confidencialidad durante y después de la impresión.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 14 de 35

- e. Las fotocopadoras, escáner, cámaras digitales o cualquier otra forma de tecnología de reproducción de PETROPERÚ, deben ser utilizados solamente por las personas autorizadas.

### **ARTÍCULO 13º: Intercambio de Software o de Información por Voz, Fax y/o Video**

**Objetivo:** Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Controlar los intercambios de información y software entre organizaciones, con observancia de la legislación legal aplicable.

**Alcance:** Todos los usuarios de PETROPERÚ.

- Los usuarios no deben dejar mensajes grabados con información confidencial, crítica o sensible, en máquinas contestadoras o sistemas de correo de voz.
- Los usuarios no deben conversar directa o telefónicamente temas sensibles, críticos o confidenciales, ante la presencia de terceros ajenos al tema, ni en lugares públicos.
- Los usuarios no deben discutir temas sensibles, críticos o confidenciales en conferencias telefónicas o videoconferencias, cuando todos los participantes no sean competentes en el tema.
- Los usuarios deben evitar, en lo posible, discutir temas sensibles, críticos o confidenciales a través de un teléfono inalámbrico o un teléfono celular.
- Los usuarios no deben enviar información confidencial, por fax u otro medio de transferencia electrónica, a menos que cuenten con la autorización del propietario de la información y del receptor previamente a la transmisión y utilice una página inicial de protección de información.


### **ARTÍCULO 14º: Transmisión de Información Confidencial, Sensible o Crítica**

**Objetivo:** Evitar la divulgación no autorizada, pérdida, modificación o mal uso de la información confidencial, sensible o crítica, generada y utilizada por personal de la organización y/o intercambiada entre Gerencias / Oficinas de PETROPERÚ y otras organizaciones o instituciones.

**Alcance:** Todo el personal de PETROPERÚ.

Está prohibido transmitir información confidencial, crítica o sensible de uso interno del Área / Operación que no haya sido debidamente autorizada por el Gerente / Superintendente / Jefe o Supervisor inmediato, o por la Gerencia General de PETROPERÚ.

### **ARTÍCULO 15º: Uso de Correo Electrónico y Adjuntos**


		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 15 de 35

**Objetivo:** Evitar la pérdida, modificación o mal uso de la información intercambiada por correo electrónico dentro de PETROPERÚ o con otras organizaciones o instituciones. Optimizar el uso del sistema de correo electrónico y sus adjuntos por parte de los usuarios del servicio.

**Alcance:** Todos los usuarios del servicio de correo electrónico de PETROPERÚ.

- a. El correo electrónico es personal e intransferible, los usuarios son responsables de todas las actividades que se realicen por medio de las cuentas de correo electrónico que les sean asignadas por PETROPERÚ.
- b. Los usuarios que tienen asignada una cuenta de correo electrónico de PETROPERÚ, deben establecer una contraseña para poder ingresar y utilizar su correo, esta clave debe ser mantenida en secreto para evitar que dicha cuenta pueda ser utilizada por otra persona.
- c. Las cuentas de correo electrónico concedidas al personal y colaboradores de PETROPERÚ, deben usarse sólo para las actividades que estén relacionadas con el cumplimiento de su función en PETROPERÚ.
- d. Está prohibido enviar por correo electrónico archivos adjuntos que no guarden relación con el quehacer de PETROPERÚ, tales como: archivos de música, video, ejecutables y, cualquier archivo de contenido pornográfico, profano o erótico y otros.
- e. Se considera como falta laboral, en concordancia con el Reglamento Interno de Trabajo, el facilitar u ofrecer la cuenta y/o buzón del correo electrónico empresarial para uso de terceras personas, darle un uso comercial o de otra naturaleza fuera de sus funciones en PETROPERÚ, distribuir mensajes con contenidos impropios y/o lesivos a la moral y realizar envíos masivos de correos no solicitados (SPAM).
- f. Los colaboradores, usuarios que no tienen la condición de trabajadores de PETROPERÚ, que faciliten u ofrezcan la cuenta y/o buzón del correo electrónico empresarial para uso de terceras personas, que le den un uso comercial o de otra naturaleza que no corresponde a las funciones que desarrolla, distribuyan mensajes con contenidos impropios y/o lesivos a la moral o realicen envíos masivos de correos no solicitados (SPAM), se les resolverá el contrato de locación de servicios o se solicitará a su empleador su relevo.
- g. Todo correo electrónico externo recibido de fuente desconocida, será eliminado en forma definitiva.
- h. El envío de información confidencial, sensible o crítica, a través del correo electrónico, deberá realizarse observando los procedimientos para transmisión de información confidencial, sensible o crítica.



		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 16 de 35


- i. El “Administrador del Sistema de Correo Electrónico” deberá mantener la privacidad, confidencialidad y seguridad de la información almacenada en el servicio de correo electrónico y, sólo la podrá levantar o hacer de conocimiento del que la solicita, con autorización del usuario o por medio de una orden judicial.

## ARTÍCULO 16º: Retención y Eliminación de Registros

**Objetivo:** Proteger los registros físicos y lógicos importantes de la organización frente a su pérdida y destrucción, en concordancia con los requisitos regulatorios, contractuales y de negocio. Asegurar que los registros y documentos vitales estén adecuadamente protegidos y mantenidos, asegurando que los registros que ya no son necesarios para PETROPERÚ y que carecen de valor, sean eliminados en el momento apropiado.

**Alcance:** Todas las Áreas / Operaciones de PETROPERÚ

- a. Todos los registros de PETROPERÚ, incluyendo expedientes y documentos electrónicos, deben ser protegidos y mantenidos adecuadamente hasta que sean necesarios, de acuerdo a lo establecido por requerimientos operativos, administrativos, legales o contractuales, conforme a lo indicado en el Cronograma de Retención de Registros.
- b. El Cronograma de Retención de Registros debe considerar, como periodos o tiempos de retención, los plazos establecidos en la normatividad de las entidades reguladoras que ejercen control o supervisión sobre PETROPERÚ. Estos registros no pueden ser eliminados o destruidos antes de culminado el periodo de retención establecido.
- c. El Área / Operación responsable –designada por Gerencia General– es la encargada de la supervisión del cumplimiento del Cronograma de Retención de Registros de su competencia, cronograma que en conjunto con los Gerentes de la Estructura Básica y Gerente Departamento Legal definirán y revisarán, estableciendo los periodos de retención para cada tipo de registro no contemplado en el inciso anterior.
- d. El Cronograma de Retención de Registros debe ser revisado y actualizado periódicamente, para garantizar que se mantiene vigente el esquema de clasificación de los requerimientos legales y plazos establecidos por PETROPERÚ.
- e. Todas las Áreas / Operaciones deben adoptar mecanismos de protección necesarios para salvaguardar la integridad, confidencialidad y disponibilidad de los registros físicos, expedientes y registros electrónicos que se encuentran bajo su custodia, de acuerdo a procedimiento.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 17 de 35

## CAPÍTULO VI: CONTROL DE ACCESOS


### ARTÍCULO 17º: Control de Accesos

**Objetivo:** Controlar el acceso a los servicios y recursos informáticos previniendo el acceso no autorizado a los mismos. Mantener los accesos autorizados a la información sobre la base de los requisitos de seguridad de la información y del negocio, considerando los procedimientos de transmisión de la información y de autorizaciones.

**Alcance:** Todos los usuarios de PETROPERÚ.

- Los propietarios de los activos de información de PETROPERÚ deben controlar el acceso tanto a la información como a los recursos de tratamiento de información y autorizar el acceso a los usuarios según los privilegios que les correspondan.
- Las áreas de Tecnologías de Información y Comunicaciones, de Oficina Principal y las Operaciones, así como las áreas usuarias, según su nivel de aprobación, deben habilitar los accesos y privilegios con perfiles estandarizados según las funciones del puesto o servicio contratado, y monitorear los registros o bitácoras de auditoría de acceso a los sistemas de información.
- Las áreas de Tecnologías de Información y Comunicaciones deberán revisar periódicamente las actualizaciones y modificaciones de los accesos otorgados, verificando que éstos estén debidamente autorizados.
- La Gerencia Departamento Tecnologías de Información y Comunicaciones, conjuntamente con las áreas de Tecnologías de Información y Comunicaciones de las Operaciones, implementarán los controles de acceso a todos los recursos informáticos bajo su control.
- Los usuarios deben cumplir con los controles de acceso implementados por PETROPERÚ y no intentar acceder a información y aplicaciones a las que no estén autorizados.
- Los usuarios deben proteger la privacidad de las contraseñas y cualquier otro mecanismo de control de acceso y autenticación a los servicios informáticos de PETROPERÚ.
- La Gerencia Departamento Tecnologías de Información y Comunicaciones deberá mantener actualizado un registro lógico y/o físico de las altas y bajas de los usuarios de los servicios y recursos informáticos de PETROPERÚ.

### ARTÍCULO 18º: Protector de Pantalla y Escritorio Limpio

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 18 de 35</b>

**Objetivo:** Evitar el acceso de usuarios no autorizados y el uso indebido de la información, que se encuentra en todos los ambientes de procesamiento de la información, para evitar su divulgación, alteración, pérdida o deterioro. Los usuarios deben ser conscientes de su responsabilidad en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad de la información puestas a su disposición.

**Alcance:** Todos los usuarios de PETROPERÚ.

- a. Los usuarios deben guardar los documentos y medios de almacenamiento de información: Disquete, CD, DVD, Memoria USB, Disco Duro Externo y otros, cuando no se estén utilizando.
- b. La información confidencial, crítica o sensible del negocio debe custodiarse en ambientes controlados que garanticen su integridad.
- c. Los usuarios deben autorizar y supervisar el uso de su estación de trabajo, cuando el personal de Soporte Técnico acceda local o remotamente al equipo.
- d. Los usuarios deben evitar la grabación de archivos importantes en el escritorio de la computadora. En caso se haga por necesidad urgente, debe ser retirado el mismo día.


#### **ARTÍCULO 19º: Uso Servicios de Red**

**Objetivo:** Prevenir el acceso no autorizado a los servicios de red, controlar el acceso a las redes internas y externas, y asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

- a) Interfaces adecuadas entre la red de la organización y la red pública o la red privada de otras organizaciones.
- b) Mecanismos adecuados de autenticación para los usuarios y los equipos.
- c) Control de los accesos de los usuarios a los servicios de información.

**Alcance:** Todos los usuarios de PETROPERÚ.

- a. Los usuarios deben contar con la autorización de su Gerente / Superintendente / Jefe de Departamento, según corresponda, para poder hacer uso de cualquiera de los servicios de red con los que cuenta PETROPERÚ.
- b. Los usuarios no deben usar los servicios de red de PETROPERÚ para ver, descargar, guardar, recibir o enviar material relacionado con:
  - i. Contenido ofensivo de cualquier clase, incluyendo material pornográfico, profano, erótico y otros.
  - ii. Promover cualquier tipo de discriminación, sea esta basada en la raza, el género, la nacionalidad, la edad, el estado civil, la orientación o preferencia sexual, la religión y/o la discapacidad.

<b>PETROPERÚ</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 19 de 35</b>


- iii. Comportamiento violento o intimidante, apuestas, juegos o beneficio económico personal.
  - iv. Archivos en cualquier formato cuyo contenido no tenga relación con las actividades propias que realiza el usuario y/o PETROPERÚ.
- c. Los usuarios deben usar el servicio de Internet con que cuenta PETROPERÚ para el cumplimiento de sus funciones. Sólo en casos extraordinarios, donde no se disponga del servicio de Internet de PETROPERÚ, se podrá usar otro servicio.
- d. Los usuarios no deben descargar o abrir archivos provenientes de Internet u otras redes externas sin tener activo y actualizado el software antivirus.
- e. Los usuarios no deben tratar de violar la seguridad de las estaciones de trabajo, servidores o cualquier otro equipo de comunicaciones de PETROPERÚ.
- f. Las áreas de Tecnologías de Información y Comunicaciones –Oficina Principal y Operaciones- deben habilitar y controlar los accesos a los servicios de red, monitorear la actividad en la red interna y desde / hacia Internet, evaluar las vulnerabilidades y, proponer a la Gerencia Departamento Tecnologías de Información y Comunicaciones los mecanismos necesarios para reforzar el cumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información.

## **ARTÍCULO 20º: Informática Móvil**

**Objetivo:** Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil: computador portátil, celular, acceso portable a datos (PDA), entre otros, que se conectan a la red interna o procesan información de PETROPERÚ.

**Alcance:** Todos los usuarios que utilizan dispositivos de informática móviles asignados por PETROPERÚ o de su propiedad.

- a. Las áreas de Tecnologías de Información y Comunicaciones realizarán una revisión del dispositivo de informática móvil y aplicarán los controles a los equipos, antes de autorizar su conexión a la red interna.
- b. Es responsabilidad del usuario, utilizando para ello las facilidades técnicas de almacenamiento recomendadas o proporcionadas o implementadas por las áreas de Tecnologías de Información y Comunicaciones, realizar periódicamente una copia de respaldo de la información confidencial, crítica o sensible contenida en sus dispositivos de informática móvil.
- c. Es responsabilidad del usuario, utilizando para ello las facilidades técnicas de cifrado proporcionadas e implementadas por las áreas de Tecnologías de Información y Comunicaciones, proteger la información confidencial del negocio

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 20 de 35</b>

que reside en los dispositivos de informática móvil para evitar su divulgación en caso de pérdida o robo.

- d. Los usuarios que utilizan dispositivos móviles de informática, deberán tener en cuenta el “Procedimiento de Seguridad de Equipos fuera de las Instalaciones de PETROPERÚ”, cuando el caso lo amerite.

## **CAPÍTULO VII: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**

**Objetivo:** Proteger la confidencialidad, autenticidad e integridad de la información. Se deberán usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

**Alcance:** Gerencia Departamento Tecnologías de la Información y Comunicaciones, áreas de Tecnologías de la Información y Comunicaciones de las Operaciones, y usuarios.

### **ARTÍCULO 21º: Adquisición y Desarrollo**

Los proyectos relacionados con tecnologías de información y comunicaciones, involucran distintas fases durante su “Ciclo de Vida”, como son: Proceso de adquisición y desarrollo de sistemas, pre-implementación, implementación, post implementación y revisión de la calidad.

En cada una de estas fases se deberá contemplar la implementación de controles lógicos de aplicación definidos en los requerimientos efectuados por los usuarios.

### **ARTÍCULO 22º: Uso de Controles Criptográficos**


- a. El uso de algoritmos de cifrado propietarios no está permitido para ningún propósito, a menos que sea revisado por personal experto y aprobado por la Gerencia Departamento Tecnologías de Información y Comunicaciones o las áreas de Tecnologías de Información y Comunicaciones de las Operaciones.
- b. La información sensible, crítica o confidencial debe ser cifrada antes de ser transmitida, en especial cuando se utilizan equipos de informática móvil fuera de las instalaciones de PETROPERÚ.

## **CAPÍTULO VIII: RECURSOS HUMANOS E INFORMACIÓN CONFIDENCIAL**

### **ARTÍCULO 23º: Protección de Datos y Privacidad de la Información Personal**


**Objetivo:** Evitar el incumplimiento de la normatividad legal aplicable, requisitos reglamentarios u obligación contractual, así como toda obligación de seguridad de la información relacionada con la privacidad de la información personal.

**Alcance:** Todos los usuarios de PETROPERÚ.

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 21 de 35</b>

- a. Todos los datos personales, como es el caso de legajos de personal, exámenes médicos, entre otros, son considerados confidenciales.
- b. La recolección de datos personales no puede hacerse por medios desleales, fraudulentos, en forma contraria a las disposiciones de la ley o sin el consentimiento del titular o persona natural a la que están referidos.
- c. Los datos personales deben utilizarse solo para los fines para los cuales han sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público o a través de la Ley de Transparencia y Acceso a la Información Pública.
- d. Los datos personales sensibles, que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, sólo pueden ser recolectados y ser objeto de tratamiento, cuando la ley lo autorice o exista mandato judicial o consentimiento del titular o cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.
- e. Los datos personales deben ser almacenados en áreas seguras: i) Físicas: restringiendo el acceso a personal no autorizado y, haciendo uso de mecanismos de protección que garanticen su privacidad, legitimidad, confidencialidad e integridad. ii) Lógicas: haciendo uso de contraseñas para el acceso a las redes, sistemas de información, aplicaciones y/o bases de datos que contengan datos personales.
- f. Las áreas de Recursos Humanos son responsables del registro de los datos personales, así como de supervisar la implantación de medidas técnicas y organizativas que resulten necesarias para garantizar la integridad y confidencialidad de los datos personales, de modo de evitar su mal uso, adulteración, pérdida, así como consulta o tratamiento no autorizado.
- g. La Gerencia Departamento Tecnologías de Información y Comunicaciones asesorará a la Gerencia Departamento Recursos Humanos, a su expresa solicitud, en la implementación corporativa de controles de seguridad de la información, usando tecnologías de información y comunicaciones propias o contratadas por PETROPERÚ.
- h. Los datos personales confidenciales o reservados, sólo podrán ser revelados por mandato judicial y/o cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

## **CAPÍTULO IX: DISPOSICIONES COMPLEMENTARIAS**

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 22 de 35

#### **PRIMERA: Aplicación Supletoria**

En todo lo no previsto expresamente en el presente reglamento, será de aplicación lo dispuesto en el Estatuto Social y/o norma aplicable a PETROPERÚ.

#### **SEGUNDA: Propuesta de Procedimientos, Formatos y Otros**

En un plazo de noventa (90) días de entrada en vigencia del presente reglamento, las Gerencias de la Estructura Básica presentaran al Comité de Seguridad de la Información sus procedimientos técnicos, formatos y otros, necesarios para la aplicación del Reglamento de Seguridad de la Información.

#### **TERCERA: Aprobación de Procedimientos, Formatos y Otros**

Los Procedimientos, para la correcta aplicación del presente reglamento, deberán ser aprobados por Gerencia General en un plazo máximo de nueve (9) meses de entrada en vigencia del Reglamento de Seguridad de la Información.

#### **CUARTA: Vigencia del Reglamento**

El presente reglamento entrará en vigencia a partir del décimo quinto (15) día útil de su aprobación.


#### **QUINTA: Difusión y Supervisión del Reglamento**

La difusión a todos los usuarios, estará a cargo de la Gerencia General, Gerencias de Estructura Básica, Gerencias y Superintendencias de la Organización Complementaria, Jefes de Departamento / Unidad / Asesoría / Oficina, y Supervisores, en forma de cascada.

El Comité de Seguridad de la Información promoverá la adecuada difusión del contenido y alcances del Reglamento, así como la supervisión de su estricto cumplimiento, para lo cual deberá orientar la capacitación a todo el personal, colaboradores y usuarios, a través de las Oficinas de Recursos Humanos y los Administradores de Contratos.

El Comité de Seguridad de la Información podrá revisar cuando se lo propongan o cuando el caso lo amerite el contenido del presente Reglamento, en coordinación con las dependencias competentes de la Empresa, y propondrá las modificaciones que correspondan, para garantizar la confidencialidad, integridad y disponibilidad de toda la información que almacena y procesa PETROPERÚ.




		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 23 de 35

## CAPÍTULO X: ANEXOS

### ANEXO 1: Glosario de Términos

- Activo de Información:**  
Recurso del sistema de información o relacionado con éste, necesario para que la organización alcance los objetivos propuestos.
- Ambiente Controlado:**  
Ambiente que puede ser de acceso restringido, donde existen controles para el ingreso de personal autorizado; o, abierto, de tal manera que esté a la vista de varias personas, evitando el ingreso de algún intruso, todo ello de acuerdo a la sensibilidad de la información que se trate.
- Análisis de Riesgos:**  
Es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir.  
  
Para el análisis de riesgos se utilizan herramientas informáticas que automatizan las actividades de identificación, evaluación, y tratamiento de los riesgos, que permiten construir un registro histórico de los eventos de incidentes que ha tenido la organización, así como indicar y dejar registradas las medidas de mitigación que se tomaron en cuenta para disminuir el impacto de las vulnerabilidades.
- Autenticación:**  
Es el proceso de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un computador o un programa del computador. En una Web, "autenticación" es un modo de asegurar que los usuarios son quién dicen ser.
- Asignación de Recursos Informáticos:**  
Es el acto por el cual se entrega, a un determinado usuario, recursos informáticos específicos, de acuerdo al pedido formulado por el área donde presta servicio. Los autorizados a formular dicha solicitud, están establecidos en el Cuadro de Niveles de Autoridad y Responsabilidad.
- Códigos Ocultos Maliciosos o Código Troyano:**  
Es un programa computacional que aparentemente es útil pero que en realidad causa daño, los cuales pueden encontrarse en las aplicaciones software sin la autorización o desconocimiento de los usuarios o los administradores de la red de datos.
- Confidencialidad de la Información:**  
Se refiere a la gradualidad de la reserva de la información por parte del dueño de esta, para que sea usada solo por personas autorizadas que indique el dueño de dicha información.
- Control:**

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 24 de 35

Política, reglamento, procedimientos, prácticas y/o estructuras organizacionales diseñadas para proporcionar una garantía razonable, que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.

**9. Control por Oposición:**

Se establece para mantener una adecuada segregación de funciones sobre una tarea o actividad, de tal forma que un usuario o un área de la organización pueda iniciar y registrar las transacciones mientras un segundo usuario o área de la gestión lo revisa de manera concurrente.

**10. Contraseña:**

Es un código o una palabra que se utiliza para acceder a datos restringidos de un ordenador. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida, y no si el usuario está autorizado a utilizar esa contraseña.

**11. Controles Criptográficos:**

Son mecanismos establecidos para controlar o proteger la integridad, confidencialidad y autenticidad de la información o comunicaciones de los usuarios en una red de datos.

**12. Correo Electrónico:**

Toda referencia al "correo electrónico" se entiende referida al correo electrónico que asigna PETROPERÚ a sus usuarios, para fines propios del ejercicio de sus funciones. Dichos correos electrónicos utilizan el dominio "petroperu.com.pe".

**13. Criptografía:**

Es la rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas. Este procedimiento permite asegurar la transmisión de informaciones privadas por las redes públicas, desordenándola matemáticamente encriptándola o cifrándola de manera que sea ilegible para cualquiera, excepto para la persona que posea la "llave" que pueda ordenar descifrar o descifrar la información nuevamente.

**14. Customisar:**

Modificar una herramienta u objeto para adaptarlo a las preferencias de un usuario o propietario, en especial de tal manera que se distinga de cualquier otro. Seleccionar las preferencias del producto o servicio físico, o contenidos de información, que desea que le sean suministrados.


**15. Cronograma Retención de Registros:**

Intervalo de tiempo que almacenamos un registro antes de eliminarlo.

**16. Empleado:**

Toda persona natural que presta servicios en PETROPERÚ, con contrato de trabajo a plazo indeterminado o a plazo fijo.

**17. Equipo Informático:**

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 25 de 35

Aquel bien que almacena, traslada y procesa información, sean éstos propios o contratados bajo cualquier modalidad por PETROPERÚ.

**18. Estación de Trabajo:**

Es el equipo –computadora personal o portátil- asignado al usuario de PETROPERÚ, conforme a los procedimientos derivados de la Política Corporativa y Reglamento de Seguridad de la Información.

**19. Herramientas de Ofimática:**

Permiten idear, crear, operar, transmitir y almacenar la información necesaria para la gestión de PETROPERÚ, tales como:

- Procesamiento de textos.
- Hoja de cálculo.
- Herramientas de presentación multimedia.
- Utilidades: agendas, calculadoras, etc.
- Programas de e-mail, correo de voz, mensajeros, dispositivos inalámbricos.
- Suite o paquete ofimático: paquete de múltiples herramientas ofimáticas como Microsoft Office, OpenOffice, etc.

**20. Información Crítica / Sensible / Confidencial:**

- **Información Crítica:** Es indispensable para la operación de PETROPERÚ.
- **Información Sensible:** Debe de ser conocida por personas autorizadas.
- **Información Confidencial:** Clasificación de alta seguridad pero de distribución limitada.

**21. Interfaz Gráfica:**

Conocida como GUI, es un programa informático que interactúa con el usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz. Su principal uso consiste en proporcionar un entorno visual sencillo, para permitir la comunicación con el sistema operativo de una estación de trabajo.

**22. Llave:**


En encriptación y firmas digitales, es un valor utilizado en combinación con un algoritmo para encriptar (cifrar) o desencriptar (descifrar) información.

**23. Log de Eventos:**

Registro escrito y permanente que recauda la información de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos informáticos.

**24. Log Servers:**

Se denomina Log Servers a los registros automáticos que realizan los servidores para almacenar datos de identificación como: procesos normales o fallidos del sistema informático, registro de horas de ingreso y salida de los usuarios al sistema informático, identificación de aplicaciones que se usaron, que fallas y en que hora ocurrieron, así como referencias a dichas fallas, entre otros.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 26 de 35

**25. No Repudio / No Rechazo:**

Es la habilidad de identificar quien ha llevado a cabo acciones desde una computadora personal, con el objetivo de que los usuarios no puedan negar las responsabilidades de las acciones que ellos llevan a cabo. Generalmente utilizado en el sentido de crear una huella de auditoria indiscutible para identificar la fuente de una transacción comercial o acciones maliciosas.

**26. Propietario Activo de Información:**

Son los Gerentes o Superintendentes de la Organización Complementaria, los Jefes de Departamento, Unidad, Planta u Oficina y los Supervisores, quienes tienen la responsabilidad de gestionar la integridad, el uso y el reporte preciso de los datos, para ejecutar y para controlar el negocio, compromiso que incluye autorizar el acceso y asegurar que estén actualizadas las reglas de acceso cuando ocurran cambios de personal o colaboradores.

**27. Recursos Informáticos:**

Referido a la generalidad de equipos informáticos (hardware) y programas de ordenador (software y sistemas de información), cuyo uso y aplicación es normado por la Gerencia Departamento Tecnologías de Información y Comunicaciones.

**28. Red de Datos:**

Consiste en la interconexión entre las estaciones de trabajo con que cuenta PETROPERU. La Red de Datos incluye tanto el hardware como el software necesarios para la interconexión de los distintos dispositivos y el tratamiento de la información.

**29. Registro o Bitácora de Auditoría:**

Registro cronológico de las actividades de un sistema para permitir la reconstrucción y el examen de las actuaciones de los usuarios en el mismo.

**30. Seguridad Física de los Recursos Informáticos y de Telecomunicaciones:**

Son las medidas de seguridad externas o físicas destinadas a proteger las instalaciones donde residen los equipos informáticos y de telecomunicaciones con que cuenta PETROPERÚ.

**31. Seguridad Informática:**

Son las técnicas desarrolladas para proteger los equipos informáticos o sistemas conectados en una red, frente a daños accidentales o intencionados.


**32. Seguridad Lógica de los Recursos Informáticos:**

Son los mecanismos destinados a proteger la información almacenada en los equipos informáticos y la transmisión de datos de PETROPERÚ.

**33. Servicio de Ofimática:**

Es el servicio que abarca el conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

**34. Sistema de Detección de Intrusos:**

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 27 de 35

Sistemas utilizados para detectar las intrusiones o los intentos de intrusión; cualquier mecanismo de seguridad con este propósito puede ser considerado un IDS, pero generalmente sólo se aplica esta denominación a los sistemas automáticos (hardware o software).

**35. Soporte Técnico:**

Es el servicio de asesoría, mantenimiento y reparación que brinda la Gerencia Departamento Tecnologías de Información y Comunicaciones a los usuarios de PETROPERÚ, en forma presencial o remota, mediante comunicaciones telefónicas, por correo electrónico o por cualquier otro medio de comunicación interna.

**36. Tratamiento de Información:**


Es una serie ordenada de operaciones realizadas sobre la información: captación, almacenamiento, clasificación, elaboración y utilización de la información.

**37. Usuario:**

Persona que cuenta con autorización para tener acceso a la información o recursos de tratamiento de la información de PETROPERÚ. Ejemplo: Miembros del Directorio, Gerente General, Gerentes de Estructura Básica y Complementaria, Trabajadores, Practicantes, Consultores, Prestadores de Servicios Profesionales, Personal de Empresas Contratistas, etc.

**38. Virus Informático**

Un virus informático es un programa creado especialmente para invadir computadores y redes y crear el caos. El daño puede ser mínimo, como hacer aparecer una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo archivos dentro de la computadora.

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 28 de 35</b>

## **ANEXO 2: Modelo de Texto de Confidencialidad y Cuidado del Ambiente para Servicio de Correo Electrónico**

El texto legal de confidencialidad será pie de página de todos los correos que se emiten con el servicio de correos de PETROPERÚ, estará redactado en español e inglés y llevará adicionalmente un mensaje sobre cuidado del ambiente.

### Aviso Legal de Confidencialidad:

Este correo y la información contenida o adjunta al mismo es privada y confidencial y va dirigida exclusivamente a su destinatario. PETROPERÚ informa a quien pueda haber recibido este correo por error que contiene información confidencial cuyo uso, copia, reproducción o distribución está expresamente prohibida.

Si no es usted el destinatario del mismo y recibe este correo por error, le rogamos lo ponga en conocimiento del emisor y proceda a su eliminación sin copiarlo, imprimirlo o utilizarlo de ningún modo.

### Privacy Disclaimer:

This mail and its attached information are private, confidential and it only has one addressee. If anybody receives this mail by error, PETROPERU informs the possible receiver that the use, copy, reproduction or distribution of it is forbidden.


Despite you are not the addressee of the e-mail and you receive it by error, we will appreciate you immediately inform the emitter and delete the mail without making a copy or impression, or use it in any way.

### Cuidado del Ambiente:

Cuidar nuestro ambiente es también tu compromiso. Imprime este mensaje y/o sus adjuntos solo si es imprescindible hacerlo. Reducir el consumo innecesario de papel es tu decisión.

### Care for the Environment:

Caring for our environment is also your commitment. Print this message and/or its attachments only if it is essential to do so. Reducing the unnecessary consumption of paper is your decision.

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 29 de 35</b>

### **ANEXO 3: Requisitos de Seguridad de la Información con Empleados, Colaboradores, Usuarios y Otros Terceros**

**3.1. *Los contratos de trabajo con empleados, convenios con practicantes, contratos de locación de servicios y otros análogos, deben contener según corresponda las siguientes cláusulas:***

- **Contratos de Trabajo:**

“Es obligación del contratado cumplir con la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ y, mantener la confidencialidad y privacidad de la información recibida, en medios impresos o en formato digital, de proveedores, organismos reguladores, socios estratégicos o comunidad vinculada, que mantengan relación con PETROPERÚ.”

“No mantener el riguroso cuidado de los activos de información de PETROPERÚ otorgados para su uso, ni avisar a tiempo de fallas en los mismos al área de Tecnologías de Información y Comunicaciones de la dependencia donde presta servicios, es considerado un incumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ.”

*Cláusula sobre privacidad y confidencialidad empresarial:*

“El contratado tiene y asume la obligación de guardar el secreto y la confidencialidad de toda la información de PETROPERÚ a la que tenga acceso en virtud del presente contrato, esta obligación subsistirá aún durante el plazo de un (1) año después de finalizada la relación laboral. El contratado será responsable de todos los daños y perjuicios que se deriven como consecuencia del incumplimiento doloso o culposo de dicha obligación”

- **Convenios de Prácticas:**


“Es obligación del practicante cumplir con la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ, guardar confidencialidad y reserva de la información a la que acceda en virtud del presente convenio, y reportar de inmediato cualquier irregularidad de seguridad de la información detectada.”

“No mantener el riguroso cuidado de los activos de información de PETROPERÚ otorgados para su uso, ni avisar a tiempo de fallas en los mismos al área de Tecnologías de Información y Comunicaciones de la dependencia donde desarrolla sus prácticas, es considerado un incumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ.”

- **Contratos con Terceros:**

“El contratista deberá cumplir con la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ, guardar confidencialidad y reserva de la información a la que acceda en virtud del presente contrato, y reportar de inmediato cualquier irregularidad de seguridad de la información detectada.”



		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 30 de 35

“No mantener el riguroso cuidado de los activos de información de PETROPERÚ otorgados para su uso, ni avisar a tiempo de fallas en los mismos al área de Tecnologías de Información y Comunicaciones de la dependencia donde suministra servicios, es considerado un incumplimiento de la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información de PETROPERÚ.”

**Nota:** Para los contratos vigentes, el Administrador del Contrato deberá cursar una comunicación adjuntando un ejemplar de la Política Corporativa, Reglamento y/o Procedimientos de Seguridad de la Información, en el último caso conforme se aprueben cuando sean de aplicación.


**3.2. La Gerencia Departamento Recursos Humanos deberá incorporar al Reglamento Interno de Trabajo las recomendaciones siguientes:**

- **Capítulo II: Derechos y Obligaciones de la Empresa, Artículo 7º**

Brindar, desde la inducción, entrenamiento y capacitación permanente sobre la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información, que permita comprender los requisitos de seguridad de la información, responsabilidades legales y controles del negocio, así como las buenas prácticas en el uso de los recursos de tratamiento de la información.

- **Capítulo IV: Obligaciones de los Trabajadores, Artículo 17º**

- a. Cumplir con la Política Corporativa, Reglamento y Procedimientos de Seguridad de la Información.
- b. Reportar cualquier incidente de seguridad de la información al Comité de Seguridad de la Información o Supervisor de Seguridad de la Información, según el procedimiento de gestión de incidencias establecido.
- c. Controlar los términos de seguridad de la información en contratos con terceros y en la relación con nuestros clientes.
- d. Velar por la seguridad de los activos de información que están a su cargo y bajo su responsabilidad, así como la del personal, colaboradores, usuarios y otros terceros, de la dependencia o área bajo su supervisión.

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 31 de 35

#### ANEXO 4: Modelo Cronograma de Retención de Registros

Relación referencial de categorización de registros, documentos y periodos de retención:

- **Ejemplo de categorización para registros o expedientes:**

- Contabilidad y Finanzas
- Documentos Electrónicos
- Expedientes Corporativos
- Correspondencia y Memorando Interno
- Contratos
- Expedientes Legales y Documentos
- Documentos de Pago
- Documentos de Pensiones
- Expedientes de Personal
- Expedientes de Impuestos

- **Ejemplo de documentos y periodos de retención:**

- Contabilidad y Finanzas:

Será determinado por la Gerencia Área Finanzas con sujeción al Artículo 16º del Reglamento.


Tipo de Registro / Expediente	Periodo de Retención
Cuentas pagadas a proveedores.	Siete (7) años
Cuentas recibidas por proveedores.	Siete (7) años
Reportes anuales de auditoría y estados financieros.	Permanente
Registros anuales de auditoría, incluyendo papeles de trabajo y otros documentos relacionados a la auditoría.	Siete (7) años después de culminada la Auditoría
Planes anuales y presupuestos.	Dos (2) años
Estados bancarios y cheques cancelados.	Siete (7) años

**Nota:** Los plazos dependerán de la norma legal o política interna en casos no legislados.

- Documentos Electrónicos:

Será determinado por las gerencias competentes con sujeción al Artículo 16º del Reglamento.


Tipo de Registro / Expediente	Periodo de Retención
Todos los e-mails recibidos y enviados fuera y dentro de PETROPERÚ serán eliminados después de un tiempo determinado.	Un (1) año
Los correos relacionados a temas de PETROPERÚ deben ser bajados a un directorio o carpeta en un servidor de red.	Permanente

		
GERENCIA GENERAL	SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.	Código: MASI-002 Elaborado: CSI
	DOCUMENTO N°2	Revisado: 15 Diciembre 2010
Comité Seguridad de la Información	REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Versión: v.1 Página: 32 de 35

PETROPERÚ retendrá a través de sus procesos de backup, los correos eliminados por los usuarios del servicio, después de ese tiempo estos correos serán eliminados definitivamente.	Seis (6) meses
--	----------------

**Nota:** No todos los correos electrónicos deben retenerse, depende del asunto del mismo.


- c. Documentos Impresos: Establecer pautas para los Archivos Centrales de OFP y las Operaciones, así como otros archivos bajo custodia de las Gerencias de Estructura Básica.
- d. Documentos en Archivos Compartidos: Establecer pautas para los lugares compartidos en la red y considerar un acápite en los Procedimientos de Seguridad de la Información.

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002</b> <b>Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1</b> <b>Página: 33 de 35</b>

#### **ANEXO 5: Transmisión de Información Confidencial, Crítica o Sensible**

El procedimiento de tratamiento de información confidencial, crítica o sensible, debe incluir:

- a) La información impresa que sea clasificada como CONFIDENCIAL, CRÍTICA O SENSIBLE, además de ser clasificada y rotulada de la misma manera en sobre cerrado, deberá ser lacrada para evitar y/o detectar su lectura y/o difusión no autorizada; asimismo, cada hoja que la contiene deberá poseer el sello de agua de CONFIDENCIAL, CRÍTICA O SENSIBLE, ello con el fin de mantener su carácter de reserva en caso sea reproducida por algún medio electrónico (fax, scanner, fotocopia, etc.)
- b) Para el caso de envío de información, clasificada como CONFIDENCIAL, CRÍTICA O SENSIBLE, entre las diferentes áreas de PETROPERÚ, por medio del sistema de correo electrónico o a través de cualquier sistema de directorio de archivos, el archivo que contiene la misma deberá ser convertido a un formato seguro que evite su modificación, copiado parcial o impresión del mismo, para ello se recomienda su conversión a formato "PDF Seguro".
- c) La información impresa que sea clasificada como CONFIDENCIAL, CRÍTICA O SENSIBLE, deberá ser guardada en archivadores independientes y exclusivos en un lugar seguro y bajo llave.
- d) Cualquier información considerada de carácter CONFIDENCIAL, CRÍTICA O SENSIBLE, solicitada por alguna organización pública o privada, externa a PETROPERÚ, deberá ser canalizada y enviada al área competente, la cual coordinará con la Gerencia General o la Gerencia de Estructura Básica, según fuere el caso, la decisión de entregarse o no.
- e) Tratándose de información requerida por la administración pública, se deberá brindar información documentada, de acuerdo a los procedimientos administrativos y/o legales establecidos.

<b>PETROPERU</b> 		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002 Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1 Página: 34 de 35</b>

## ANEXO 6: Composición del Comité de Seguridad de la Información

### Miembros del Comité de Seguridad de la Información:

Presidente	Representante 1 de Gerencia General
Suplente	Representante 2 de Gerencia General
Miembro	Representante 1 de Gerencia Operaciones Talara
Suplente	Representante 2 de Gerencia Operaciones Talara
Miembro	Representante 1 de Gerencia Operaciones Oleoducto
Suplente	Representante 2 de Gerencia Operaciones Oleoducto
Miembro	Representante 1 de Gerencia Operaciones Selva
Suplente	Representante 2 de Gerencia Operaciones Selva
Miembro	Representante 1 de Gerencia Operaciones Conchan
Suplente	Representante 2 de Gerencia Operaciones Conchan
Miembro	Representante 1 de Gerencia Operaciones Comerciales
Suplente	Representante 2 de Gerencia Operaciones Comerciales
Miembro	Representante 1 de Gerencia Área Producción y Planeamiento
Suplente	Representante 2 de Gerencia Área Producción y Planeamiento
Miembro	Representante 1 de Gerencia Área Finanzas
Suplente	Representante 2 de Gerencia Área Finanzas
Miembro	Representante 1 de Gerencia Departamento Legal
Suplente	Representante 2 de Gerencia Departamento Legal
Miembro (*)	Gerente Departamento Tecnologías de Información y Comunicaciones
Miembro (*)	Jefe Unidad Seguridad OFP
Coordinador (**)	Representante Departamento Tecnologías de Información y Comunicaciones, quien participará del Comité con voz pero sin voto.


### Equipo Interno de Seguridad de la Información:

Compuesto por un (1) representante de cada una de las áreas de Tecnologías de Información y Comunicaciones de las Operaciones, y el Supervisor de Seguridad de la Información de OFP, quienes participan del Comité con voz pero sin voto.

### Asesor Externo o Consultor Independiente en Seguridad de la Información:

El Comité, si lo estima conveniente, podrá contar en sus reuniones con un (1) Asesor Externo en Seguridad de la Información o Consultor Independiente en Seguridad de la Información, quien participará del Comité con voz pero sin voto.

(\*) Designación al cargo

		
<b>GERENCIA GENERAL</b>	<b>SEGURIDAD DE LA INFORMACIÓN DE PETROPERÚ S.A.</b>	<b>Código: MASI-002</b> <b>Elaborado: CSI</b>
	<b>DOCUMENTO N°2</b>	<b>Revisado: 15 Diciembre 2010</b>
<b>Comité Seguridad de la Información</b>	<b>REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Versión: v.1</b> <b>Página: 35 de 35</b>

(\*\*) Designado por el Gerente Departamento Tecnologías de Información y Comunicaciones; y, a su vez cumple la función de Secretario del Comité.

El Presidente y los Miembros titulares, así como los suplentes, salvo los representantes de la Gerencia Departamento Tecnologías de Información y Comunicaciones, y la Unidad Seguridad de Oficina Principal, serán renovados cada dos (2) años. La designación es hecha por Gerencia General.