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

ÍNDICE

Fecha:

I. OBJETIVO

Brindar lineamientos claros y entendibles para el adecuado cumplimiento de los controles de Seguridad de la Información del Anexo A de la norma "NTP-ISO/IEC 27001:2014 Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición", que implica entre otros aspectos:

- Asegurar una apropiada salvaguarda de todos los activos (información, otros activos asociados con información e instalaciones de procesamiento de información) en adelante "activos de información" de PETROPERÚ.
- Aplicar eficientemente los controles de Seguridad de la Información.

II. BASE NORMATIVA

2.1. Normas Legales

- Resolución Ministerial Nº 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 Nº 166-2017-PCM del 20.06.2017, donde se modifica el artículo 5 de la Resolución Ministerial Nº 004-2016-PCM.
- 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.
- Norma Técnica Peruana NTP-ISO/IEC 27002:2017 Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición.
- Política Nacional de Gobierno Electrónico

2.2. Normas Internas

- Política Corporativa de Seguridad de la Información de PETROPERÚ.
- Política Corporativa de Protección de Datos Personales.
- Código de Buen Gobierno Corporativo de PETROPERÚ.
- Código de Integridad de PETROPERÚ.
- Reglamento de Organización y Funciones (ROF) de PETROPERÚ.
- Reglamento Interno de Trabajo de PETROPERÚ.
- Reglamento Interno del Comité de Buenas Prácticas de Gobierno Corporativo de PETROPERÚ.
- Normas sobre Conflicto de Intereses de PETROPERÚ.
- Manual de Organización y Funciones (MOF) de PETROPERÚ.
- Estatuto Social de PETROPERÚ.

III. ALCANCE Y RESPONSABILIDAD

El presente Reglamento será de aplicación general y obligatoria para Miembros del Directorio, Gerente General, Gerentes, Gerentes Departamento, Personal en General, Practicantes (en sus dos modalidades), Prestadores de locación de Servicios, Personal destacado de Contratistas y otros, en adelante denominados "usuarios", que requieran tener acceso a la información o recursos de la información

de PETROPERÚ, mientras desempeñen sus labores en la misma o brinden servicios, y que exista vínculo laboral o civil, y de acuerdo a convenios o norma específica, incluso al cese de sus funciones.

La información y los medios para su generación, tratamiento, transmisión y almacenamiento, son activos de información importantes de la Empresa y por ello, requieren ser protegidos. La confidencialidad, integridad y disponibilidad de la información, son esenciales para viabilizar la competitividad, rentabilidad, integridad, ética y transparencia de PETROPERÚ.

La información, en cualquiera de sus medios (físico o digital); es cada vez más esencial en los procesos de negocio para conseguir eficazmente los objetivos a corto, mediano y largo plazo, para mantener la rentabilidad y competitividad, gestionar adecuadamente los recursos internos y externos, obtener y mantener clientes y cuota del mercado; así como, gestionar y mantener el conocimiento; está expuesta a diversas amenazas y vulnerabilidades crecientes (incluyendo fraudes informáticos, fallo electrónico, espionaje, error humano, sabotaje, vandalismo, incendios, inundaciones, virus informáticos, ataques de intrusión o denegación de servicios, cada vez más frecuentes y sofisticados); por tanto, deberá protegerse adecuadamente, cualquiera que sea la forma que tome o los medios por los que se comparta o almacene en todas las instalaciones a nivel nacional de PETROPERÚ.

Para lograr este fin, es necesario contar con un documento normativo, el cual se ha redactado de una manera clara y concisa, para comprensión y aplicación de todos los usuarios, con la finalidad de educar y capacitar en forma clara y detallada sobre la gestión de la Seguridad de la Información.

La Dependencia responsable de dirigir, controlar, validar y cumplir con la implementación de los controles y planes de acción de seguridad de la información es la Gerencia Auditoría Interna y Riesgos; y de su aprobación es la Gerencia General.

IV. DEFINICIONES

Las definiciones se pueden ver en el Anexo 1.

V. DESARROLLO DEL DOCUMENTO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN (NTP-ISO/IEC 27001-A.5)

5.1. Dirección de la Gerencia para la Seguridad de la Información (NTP-ISO/IEC 27001-A.5.1)

Proporcionar orientación de gestión y apoyo a la Seguridad de la Información de acuerdo con los requerimientos de PETROPERÚ, y las leyes y regulaciones pertinentes.

5.1.1. Política para la Seguridad de la Información (NTP-ISO/IEC 27001-A.5.1.1)

- Las directivas y requerimientos necesarios para implementar un nivel razonable de protección de los activos de información de PETROPERÚ están plasmadas en la *Política Corporativa de Seguridad de la Información* y *Política Corporativa de Protección de Datos Personales*.
- Las Políticas de Seguridad de la Información deben ser aprobadas por el Directorio, publicadas en la Intranet Corporativa y la Página Web Institucional; asimismo, difundidas a las diferentes Dependencias de PETROPERÚ. Estas Políticas se deben elaborar según el *lineamiento Elaboración de Políticas Corporativas – LA1-ADM-007*.

5.1.2. Revisión de las Políticas de Seguridad de la Información (NTP-ISO/IEC 27001-A.5.2)

- Se deben realizar revisiones y mantenimiento de las *Políticas de Seguridad de la Información* cada dos (02) años o cuando ocurran cambios significativos.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (NTP-ISO/IEC 27001- A.6)

5.2. Organización Interna (NTP-ISO/IEC 27001-A.6.1)

PETROPERÚ tiene establecido el siguiente marco de gestión para realizar y controlar la implementación y operación de la Seguridad de la Información.

5.2.1. Funciones y responsabilidades para la Seguridad de la Información (NTP-ISO/IEC 27001-A.6.1.1)

Las funciones y responsabilidades para la Seguridad de la Información se asignan de la forma siguiente:

A. Directorio

- Aprobar la Política Corporativa de Seguridad de la Información, Política Corporativa de Protección de Datos Personales y sus modificaciones.
- Delegar al Gerente General la aprobación de los documentos normativos.

B. Gerente General

- Aprobar el Reglamento de Seguridad de la Información y sus modificaciones, así como otros documentos normativos complementarios que el Comité de Seguridad de la Información proponga según su competencia.
- Aprobar la asignación de los recursos necesarios para implementar, mantener y mejorar adecuadamente la Seguridad de la Información.
- Designar al Oficial del Seguridad de la Información.

- Constituir y Designar a los miembros del Comité de Seguridad de la Información.
- Evaluar la implementación, mantenimiento y desempeño de la Gestión de la Seguridad de la Información.

C. Comité Seguridad de la Información

- PETROPERÚ tiene un Comité de Seguridad de la Información, designado por el Gerente General el cual está conformado por:

Presidente (*)	Representante del titular de la Entidad.	Gerente Innovación, Desarrollo y Nuevos Negocios.
Miembro (*)	Responsable de administración o quien haga sus veces.	Gerente Gestión de Personas.
Miembro (*)	Responsable de planificación o quién haga sus veces.	Gerente Planeamiento y Gestión.
Miembro (*)	Responsable del área legal o quien haga sus veces.	Gerente Legal.
Miembro (*)	Responsable del área de informática o quien haga sus veces.	Gerente Departamento Tecnologías de Información.
Miembro (*)	Oficial de Seguridad de la Información.	Gerente Auditoría Interna y Riesgos.

(*) Designación al cargo.

- Este Comité tiene las siguientes funciones y responsabilidades:
  - Proponer la política y objetivos de Seguridad de la Información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de Seguridad de la Información.
  - Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.
  - Promover la gestión de Seguridad de la Información en los procesos y cultura organizacional.
  - Sustentar y solicitar la asignación del personal y recursos necesarios para la implementación de la Seguridad de la Información.
  - Difundir la importancia de una efectiva gestión de Seguridad de la Información a las partes interesadas.
  - Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.

D. Oficial de Seguridad de la Información

- Desarrollar la estrategia de Seguridad de la Información; vigilar el programa y las iniciativas de seguridad de la Información, y coordinar con los dueños del proceso de negocio para una alineación constante con la Norma Técnica Peruana NTP-ISO/IEC 27001.
- Garantizar que se realicen las evaluaciones de riesgos de Seguridad de la Información e impacto al negocio.
- Desarrollar estrategias de mitigación de riesgos de Seguridad de la Información.
- Hacer cumplir las regulaciones y las políticas de Seguridad de la Información.
- Monitorear la utilización y la eficiencia de los recursos de seguridad.
- Desarrollar e implementar enfoques de monitoreo y métricas de Seguridad de la Información.
- Dirigir y monitorear las actividades de seguridad de la Información.
- Desarrollar tanto métodos para captar y difundir el conocimiento, en materia de Seguridad de la Información, como métricas para determinar su eficacia y la eficiencia.
- Comunicarse con otros proveedores de aseguramiento de la Información.
- Garantizar que se identifiquen y resuelvan las brechas, vacíos y superposiciones, respecto a la Norma Técnica Peruana NTP-ISO/IEC 27001.
- En tanto el Comité no nombre a un Secretario, el Oficial de Seguridad de la Información, coordina la agenda de las sesiones del Comité de Seguridad de Información, registra y custodia las actas de estas sesiones.

E. Gerencia Auditoría Interna y Riesgos

- Dirigir y controlar los planes de acción para implementar la Seguridad de la Información.
- Validar la correcta ejecución de la Seguridad de la Información en las diferentes Dependencias de la Empresa.
- Dirigir las evaluaciones para identificar riesgos de Seguridad de la Información en todos los procesos relevantes de la Empresa.
- Dirigir la elaboración de estrategias preventivas y correctivas ante los riesgos identificados, así como controlar su cumplimiento.
- Fomentar una cultura de gestión de riesgos a nivel corporativo, a fin de identificar y prevenir los riesgos a los que la Empresa está expuesta.

F. Gerentes Nivel 2

- Asegurar en sus respectivas Dependencias la difusión de la Política Corporativa de Seguridad de la Información, la Política Corporativa de Protección de Datos Personales, el Manual, el Reglamento, los Procedimientos y los Lineamientos de Seguridad de la Información, verificando su entendimiento y controlando su cumplimiento.
- Designar al personal de sus respectivas Dependencias que debe encargarse de identificar, evaluar y dar respuesta a los riesgos de Seguridad de la Información que podrían afectar los procesos relevantes y bancos de datos personales que están bajo su responsabilidad.
- Asignar personal y otros recursos que se requieran, para el seguimiento de la implementación de los planes de tratamiento de riesgos de Seguridad de la Información, que hayan sido asignados a sus respectivas Dependencias.

G. Gerencia Departamento Tecnologías de Información

- Controlar en forma oportuna los requerimientos de necesidad de las áreas funcionales en relación a las aplicaciones informáticas y a servicios tecnológicos, cuando exista un incidente de Seguridad de la Información.
- Monitorear y controlar el cumplimiento de los niveles de servicio de los contratos de tercerización de Tecnologías de Información, en lo referente a Seguridad Informática incluida en los mismos.
- Participar de las tareas de aseguramiento de calidad de los requisitos de Seguridad, sobre proyectos, aplicaciones, infraestructura y servicios asociados a las TIC.
- Monitorear y mantener los inventarios de hardware y software actualizados, con el objeto de identificar los riesgos de Seguridad de la Información.
- Gestionar la Infraestructura (en cuanto a Hardware, Software, Redes de datos y Telecomunicaciones, Salas de Servidores y Comunicaciones), a fin de salvaguardar los activos de información.
  Dar cumplimiento a la normatividad en cuanto a Seguridad Informática establecido por la Norma ISO/IEC 27002:2013; y por la Política de Seguridad de la Información de PETROPERÚ.

H. Propietarios de Riesgos

- Apoyar en la difusión de las políticas y normas de Seguridad de la Información al personal bajo su cargo.
- Coordinar la implementación y el mantenimiento de los controles para el tratamiento de los riesgos de Seguridad de la Información según corresponda.

- Suscribir la matriz de riesgos y matriz de planes de tratamiento de riesgos según corresponda.
- Asumir responsabilidad de los controles implementados para tratar los riesgos asociados a dichos activos de información.

I. Propietarios de Activos de Información

- Velar por la seguridad de los activos de información que están a su cargo.
- Gestionar la implementación y el mantenimiento de los controles para el tratamiento de riesgos que pueden afectar los activos de información.
- Asegurar que los activos de información sean inventariados, clasificados y protegidos adecuadamente.
- Garantizar el manejo adecuado de los activos de información.

J. Usuarios (Todo personal de la Empresa)

- Proponer alternativas de mejoras en la Seguridad de la Información.
- Reportar cualquier incidente de Seguridad de la Información según procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Incluir cláusulas de confidencialidad y de Seguridad de la Información, en las condiciones técnicas de contratación de los procesos de contratación de servicios y obras.
- Asumir responsabilidad en la generación, tratamiento, transmisión y almacenamiento de los activos de información que usan en el ejercicio de sus funciones y actividades.

K. Terceros

- Cumplir las cláusulas incluidas dentro de los contratos referidas a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de PETROPERÚ.
- Proporcionar todas las facilidades necesarias para que PETROPERÚ revise el cumplimiento de las condiciones relacionadas a Seguridad de la Información, incluidas en los contratos.

Todo el personal de la Empresa, así como, personal destacado de contratistas que brinde servicios a la Empresa, debe cumplir con la *Política Corporativa de Seguridad de la Información*; la *Política Corporativa de Protección de Datos Personales, el Reglamento, los Procedimientos y demás normas de Seguridad de la Información* de PETROPERÚ.

5.2.2. Segregación de funciones (NTP-ISO/IEC 27001-A.6.1.2)

- Todo Jefe o nivel superior debe solicitar los accesos para su personal, alineado a sus labores, funciones o necesidad operativa; evitando cualquier conflicto de segregación de funciones, de ser

necesario debe elaborar una matriz de segregación de funciones según el *lineamiento Segregación de Funciones – LA1-GCPL-002*.

5.2.3. Contacto con autoridades (NTP-ISO/IEC 27001-A.6.1.3)

- En caso de incidentes de Seguridad de la Información que no puedan ser resueltos internamente y sus consecuencias lo ameritan, el Oficial de Seguridad de la Información debe informar el incidente a los contactos externos en Seguridad de la Información como la Secretaría de Gobierno Digital - SeGDI, Sistema de Coordinación de Emergencias en Redes Telemáticas – PeCERT, Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, Dirección Nacional de Inteligencia – DINI, entre otros.

5.2.4. Contacto con grupos de interés especial (NTP-ISO/IEC 27001-A.6.1.4)

- El personal involucrado en la gestión de Seguridad de la Información debe registrarse en foros de entidades o instituciones especializadas en Seguridad de la Información, por ejemplo: ISACA (Information Systems Audit and Control Association), Riesgo Cero, entre otros, a fin de que, entre otros aspectos, nos proporcionen información relevante sobre Seguridad de la Información y que nos puedan prestar apoyo en caso de incidentes de Seguridad de la Información.

5.2.5. Seguridad de la Información en la Gestión de Proyectos (NTP-ISO/IEC 27001-A.6.1.5)

- La Seguridad de la Información debe ser tratada en la Gestión de Proyectos de PETROPERÚ para garantizar que los riesgos de Seguridad de la Información son identificados y tratados como parte de los proyectos que se ejecutan en la Empresa.

5.3. Dispositivos Móviles (NTP-ISO/IEC 27001-A.6.2)

Garantizar la seguridad en el uso de dispositivos móviles.

5.3.1. Política de Dispositivos Móviles (NTP-ISO/IEC 27001-A.6.2.1)

- La Gerencia Departamento Tecnologías de Información debe llevar un registro de dispositivos móviles (asignados por PETROPERÚ).
- Todos los usuarios que usan dispositivos móviles de la Empresa deben verificar que estos hayan sido registrados ante la Gerencia Departamento Tecnologías de Información.
- Los usuarios que utilicen computadoras portátiles para el cumplimiento de las funciones asignadas deben mantener el equipo asegurado con dispositivos de seguridad (cadena de seguridad) cuando estos se encuentren desatendidos.
- No se debe asignar a los usuarios de dispositivos móviles el “rol de administrador” sobre estos dispositivos.

- Todos los dispositivos móviles deben usar la última versión formal y soportada del software, proveniente del fabricante; previa evaluación por parte del personal de la Gerencia Departamento Tecnologías de Información. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Para el cifrado o encriptado seguro de los dispositivos y las conexiones de comunicación, se tiene implementado lo siguiente:
  - Discos duros de los equipos de trabajo (laptops) proporcionados a los usuarios con la activación de la funcionalidad del "bitlocker" (habilitado para el Sistema Operativo Windows 10 Pro), con un algoritmo de cifrado de XTS-AES (estándar de cifrado avanzado) con fuerza de cifrado de 128 o 256 bits.
  - Para la transferencia de información en servicios de telefonía y videoconferencia.
  - En la conexión remota de los usuarios a la red local mediante acceso VPN (red privada virtual).
- Se debe mantener actualizado el software antivirus de los dispositivos móviles, según el *lineamiento Protección Contra Código Malicioso – LINA1-058*.

5.3.2. Teletrabajo (NTP-ISO/IEC 27001-A.6.2.2)

- La comunicación desde los equipos utilizados en la modalidad de teletrabajo a los servicios TIC que se brindan desde la red interna de PETROPERÚ, se debe realizar a través de mecanismos seguros que permitan evitar intentos de robo o interceptación de la información, asegurando el tránsito de ésta. Se sugiere el uso de VPN (redes privadas virtuales) con protocolos de seguridad como SSL (Secure Socket Layer) e IPSEC (Internet Protocol Security) o de proxy reverso, entre otros mecanismos de comunicación segura.
- Para el acceso al servicio VPN se debe seguir las directivas indicadas en el numeral 5.10.2 Acceso a redes y servicios de red.
- Los usuarios son responsables de realizar el respaldo de su información de manera periódica, ya sea en la red o en discos duros externos portátiles o equipos similares, los cuales deben ser almacenados en un sitio seguro, por lo menos cada dos semanas.
- Los usuarios deben tomar medidas para evitar discutir información confidencial por teléfono. De igual manera, deben abstenerse de dejar información confidencial en sistemas reproductores de voz, a menos que las máquinas contestadoras o sistemas de correo de voz (Buzón de voz) estén protegidos por contraseña.
- Después de completar su sesión remota, los usuarios deben cerrar las sesiones en los aplicativos a los cuales tuvo acceso y cerrar la sesión en el mecanismo de comunicación segura que haya utilizado.

SEGURIDAD DE LOS RECURSOS HUMANOS (NTP-ISO/IEC 27001-A.7)

5.4. ANTES DEL EMPLEO (NTP-ISO/IEC 27001-A.7.1)

5.4.1. Selección (NTP-ISO/IEC 27001-A.7.1.1)

- Para la selección de los colaboradores de PETROPERÚ la Gerencia Gestión de Personas debe seguir las directivas del *procedimiento Contrataciones del Personal – PROA1-072*.

5.4.2. Términos y Condiciones de Empleo (NTP-ISO/IEC 27001-A.7.1.2)

- Todo candidato a empleo en PETROPERÚ deberá suscribir el Anexo 4 "Declaraciones Juradas Contratación de Personal" del *procedimiento Contrataciones del Personal – PROA1-072* que especifica las responsabilidades de Seguridad de la Información, igualmente se especifica en la *Descripción de Puesto* que ocupará el personal a contratar.
- Incluir en los contratos de trabajo las cláusulas de cumplimiento obligatorio de la Política Corporativa y Reglamento de Seguridad de la Información, que se indican en el Anexo 2*, referente a contratos con Trabajadores.*

5.5. DURANTE EL EMPLEO (NTP-ISO/IEC 27001-A.7.2)

5.5.1. Responsabilidades de la Gerencia Nivel 2 (NTP-ISO/IEC 27001-A.7.2.1)

- PETROPERÚ establece el cumplimiento de funciones de Seguridad de la Información en la *Descripción de Puesto* de sus trabajadores y en cláusulas incluidas en los contratos con terceros, según lo establecido en el *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710*.

5.5.2. Conciencia, educación y capacitación de Seguridad de la Información (NTP-ISO/IEC 27001-A.7.2.2)

- Todos los trabajadores que ingresan a la Empresa deben participar del Programa de Inducción, que contemplan entre otros temas, la Seguridad de la Información. Este programa está a cargo de la Gerencia Gestión de Personas, según procedimiento *Inducción de Personal - PROA1-103*.
- Se debe difundir de manera quincenal, vía correo electrónico, los "tips" sobre diferentes aspectos de Seguridad de la Información.
- Se debe realizar capacitación para el personal de las diferentes Dependencias, en temas de Seguridad de la Información de acuerdo al *lineamiento Formulación del Programa de Capacitación en Seguridad de la Información – LA1-GGR-715*.

5.5.3. Procesos Disciplinarios (NTP-ISO/IEC 27001-A.7.2.3)

- Cuando se detecten presuntas infracciones respecto a Seguridad de la Información por parte de los empleados, las Dependencias involucradas deben iniciar un proceso formal de investigación para determinar responsabilidades y establecer las acciones

disciplinarias que correspondan aplicar. Los responsables de las Dependencias informarán a los empleados implicados, sobre el inicio formal del proceso disciplinario, teniendo en cuenta el *Reglamento Interno de PETROPERÚ* y el *procedimiento Aplicación de Medidas Disciplinarias – PROA1-076 v2*.

5.6. TÉRMINO O CAMBIO DE EMPLEO (NTP-ISO/IEC 27001-A.7.3)

5.6.1. Término o cambio de las responsabilidades de empleo (NTP-ISO/IEC 27001-A.7.3.1)

- Para la Terminación de la relación laboral o cambio de puesto de trabajo del colaborador, la Gerencia Gestión de Personas debe coordinar con el Jefe del colaborador y de ser necesario con el Oficial de Seguridad de la Información para definir e informar a los empleados involucrados sobre las responsabilidades y deberes de Seguridad de la Información, que deben continuar cumpliendo, luego de ser cesados o cambiados de puestos de trabajo.
- Cada dependencia debe definir e incluir, cuando sea pertinente, en los contratos con terceros las responsabilidades y deberes de Seguridad de la Información que deben continuar cumpliendo luego del término de sus servicios.
- Al término del empleo debe incluir el retorno de los activos de información proporcionados por PETROPERÚ al personal o tercero (de ser el caso) para el desempeño de las funciones asignadas, de acuerdo a lo señalado en la *circular Modificación constancia de devolución de credenciales, accesos electrónicos y otros – RRHH-ECOM-008-2013*.

GESTIÓN DE ACTIVOS (NTP-ISO/IEC 27001-A.8)

5.7. RESPONSABILIDADES POR LOS ACTIVOS (NTP-ISO/IEC 27001-A.8.1)

PETROPERÚ debe registrar y mantener actualizados sus Activos de Información, así como, definir las responsabilidades de protección apropiadas.

5.7.1. Inventario de activos (NTP-ISO/IEC 27001-A.8.1.1)

- Para elaborar y mantener un inventario de activos de información, se debe seguir las directivas del lineamiento *Identificación, Evaluación y Respuesta a los Riesgos de Seguridad de la Información – LINA1-025*.

5.7.2. Propiedad de los activos (NTP-ISO/IEC 27001-A.8.1.2)

- Cada uno de los activos de información deben tener un “propietario”, quien debe ser responsable de asegurar su apropiada clasificación y protección. PETROPERÚ es el dueño de los activos de información de la organización, y delega dicha propiedad a los Usuarios, con la finalidad de que se hagan cargo de la protección y uso adecuado de los mismos, para mejorar la eficiencia en la administración de la Seguridad de la Información.

5.7.3. Uso aceptable de los activos (NTP-ISO/IEC 27001-A.8.1.3)

- El uso de todos los activos de información debe ser con el propósito expreso de realizar tareas relacionadas a las actividades de PETROPERÚ.
- Los activos de información deben ser utilizados dentro de un adecuado entorno de seguridad de acuerdo a lo definido en la *Política Corporativa de Seguridad de la Información*, cualquiera sea el medio que lo soporte y el ambiente tecnológico en que se procesen.

5.7.4. Retorno de activos (NTP-ISO/IEC 27001-A.8.1.4)

- La finalización del empleo debe incluir el retorno de los activos de información proporcionados por PETROPERÚ al personal o tercero (de ser el caso) para el desempeño de las funciones asignadas, de acuerdo a lo señalado en la *circular Modificación constancia de devolución de credenciales, accesos electrónicos y otros – RRHH-ECOM-008-2013*.

5.8. CLASIFICACIÓN DE INFORMACIÓN (NTP-ISO/IEC 27001-A.8.2)

Los usuarios de PETROPERÚ deben asegurar que la información recibe el nivel apropiado de protección.

5.8.1. Clasificación de la Información (NTP-ISO/IEC 27001-A.8.2.1)

- Toda información que posea PETROPERÚ, se clasifica en Confidencial y Pública, según el Lineamiento *Clasificación de la Información – LA1-GCGR-702*.

5.8.2. Etiquetado de la información (NTP-ISO/IEC 27001-A.8.2.2)

- Teniendo en cuenta la clasificación de la información mencionada en el numeral 5.8.1., Los propietarios de activos deben asegurar que los activos de información de tipo confidencial estén etiquetados, de tal manera que se identifique en qué nivel de clasificación se encuentran, según el lineamiento *Clasificación de la Información – LA1-GCGR-702.*

5.8.3. Manejo de activos (NTP-ISO/IEC 27001-A.8.2.3)

- El manejo de los activos de la información debe estar de acuerdo a su clasificación según el Lineamiento *Clasificación de la Información – LA1-GCGR-702*.
- Todo activo de información de PETROPERÚ debe tener un "propietario" quien será el encargado de establecer los niveles de protección.

5.9. MANEJO DE LOS MEDIOS (NTP-ISO/IEC 27001-A.8.3)

5.9.1. Gestión de medios removibles (NTP-ISO/IEC 27001-A.8.3.1)

- Para la gestión de medios removibles se debe seguir las directivas según el *procedimiento Autorización por Excepción para Habilitar Puertos de Equipos de Cómputo – PA1-TIC-021*.

- El control de cintas correspondientes al respaldo de información se debe realizar según lo especificado en el *procedimiento Ingreso y Salida de Maletines con Cintas Magnéticas de Backup – PA1-DIN-002*.

5.9.2. Desecho de los medios (NTP-ISO/IEC 27001-A.8.3.2)

- Antes de desechar cualquier medio magnético, debe eliminarse cualquier tipo de información contenida en los mismos, de acuerdo al *procedimiento Retención y Eliminación de Registros de Información – PA1-GGR-712*.
- La disposición final de cualquier medio debe hacerse de acuerdo a la norma de los fabricantes o de los expertos correspondientes.

5.9.3. Transporte de medios físicos (NTP-ISO/IEC 27001-A.8.3.3)

- Para el transporte de medios físicos en la Oficina Principal de PETROPERÚ se deben cumplir las directivas del procedimiento *Ingreso y Salida de Maletines con Cintas Magnéticas de Backup – PA1-DIN-002*. Para el caso de documentos en papel, se debe cumplir las directivas de los Procedimientos Recepción de Correspondencia – PROA1-080, y Recepción y Entrega de Correspondencia Interna – PA1-ADM-461.

CONTROL DE ACCESO (NTP-ISO/IEC 27001-A.9)

5.10. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO (NTP-ISO/IEC 27001-A.9.1)

5.10.1. Política de Control de Acceso (NTP-ISO/IEC 27001-A.9.1.1)

- Para el registro de los accesos a los diferentes servicios de Tecnologías de la Información (TIC) con los que cuenta la Empresa se debe seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176*, este registro es revisado, aprobado y actualizado siguiendo las directivas del procedimiento *Revalidación de Accesos de los Usuarios – PROA1-154*.
- La Asignación de equipos de cómputo se debe realizar en base a una segmentación de usuarios considerando el puesto y actividades del mismo, por lo cual se debe asignar un solo equipo de cómputo (sin excepción).
- La cantidad de impresoras se debe segmentar según tipo y cantidad de usuarios que acceden a la misma, con el fin de asignar según su uso.
- Para la gestión de requisitos de seguridad de aplicaciones se debe seguir las directivas indicadas en el numeral 5.25.1. Análisis y especificaciones de requisitos de Seguridad de la Información.
- Para la protección de la Información se deben seguir las directivas del *Lineamiento Clasificación de la Información – LA1-GCGR-702*.

5.10.2. Acceso a redes y servicios de red (NTP-ISO/IEC 27001-A.9.1.2)

- Para la autorización a los accesos de red y los servicios de red se debe seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.
- Los usuarios no deben usar los servicios de red de PETROPERÚ para ver, descargar, guardar, recibir o enviar material relacionado con:
  - Contenido ofensivo de cualquier clase, incluyendo material pornográfico, erótico y otros.
  - Promover cualquier tipo de discriminación, basada en la raza, género, nacionalidad, edad, estado civil, orientación o preferencia sexual, religión o discapacidad.
  - Comportamiento violento o intimidante, apuestas, juegos o beneficio económico personal.
  - Archivos en cualquier formato cuyo contenido no tenga relación con las funciones propias que realiza el usuario o PETROPERÚ.
- 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, previa autorización de sus respectivas Gerencias.
- Los usuarios no deben descargar o abrir archivos provenientes de Internet u otras redes externas sin tener activo y actualizado el software antivirus.
- Los usuarios no deben tratar de violar la seguridad de las estaciones de trabajo, servidores o cualquier otro equipo de comunicaciones de PETROPERÚ.
- Para la conexión de equipos a la red se debe:
  - Limitar a cinco (5) el número de intentos fallidos de conexión, luego de lo cual el usuario debe quedar deshabilitado por un periodo de treinta (30) minutos.
  - Limitar el tiempo de la conexión sin actividad de acuerdo a las aplicaciones a quince (15) minutos, cuando el activo se encuentra desatendido, luego del cual el usuario deberá autenticarse nuevamente.
  - Contar con identificadores de los equipos que se conectan a la red.
- Para controlar el ingreso, salida y uso de equipos de cómputo particulares en las instalaciones se debe seguir las directivas del *Procedimiento Ingreso, salida y uso de equipo de cómputo particular – PA1-GGR-706*.
- Las redes IT (Information Technology) y OT (Operational Technology) deben estar separadas físicamente en dos redes, se debe garantizar la unidireccionalidad (OT -> IT) y solo proporcionar la Información OT que debe ser gestionada por IT, para lo cual se debe considerar el uso de dispositivos de Seguridad Informática

que eviten el acceso directo entre usuario de redes TI y OT, como Firewall, Diodo de datos, entre otros.

GESTIÓN DE ACCESO DE USUARIO (NTP-ISO/IEC 27001-A.9.2)

5.10.3. Registro y baja de usuarios (NTP-ISO/IEC 27001-A.9.2.1)

- Para el registro y baja de usuarios se debe seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.

5.10.4. Gestión de acceso a usuario (NTP-ISO/IEC 27001-A.9.2.2)

- Para la gestión de accesos se debe seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.

5.10.5. Gestión de derechos de acceso privilegiados (NTP-ISO/IEC 27001-A.9.2.3)

- La asignación de derechos de acceso privilegiados (por ejemplo: rol Administrador, root, entre otros) será efectuada por la Jefatura del personal que tendrá este tipo de acceso, en coordinación con los dueños de los activos de información o la Gerencia Departamento Tecnologías de Información, según corresponda.

5.10.6. Gestión de información de autentificación secreta de usuarios (NTP-ISO/IEC 27001-A.9.2.4)

- Para la autentificación secreta de los usuarios se debe seguir las directivas del *lineamiento Gestión de Contraseñas – LINA1-086*.

5.10.7. Revisión de derechos de acceso de usuarios (NTP-ISO/IEC 27001-A.9.2.5)

- Para la revisión de los derechos de accesos de los usuarios a los recursos informáticos de PETROPERÚ se deben seguir las directivas del procedimiento *Revalidación de Accesos de los Usuarios – PROA1-154*, bajo la responsabilidad de los niveles de aprobación definidos en el Anexo 1 del mencionado procedimiento y las consecuencias que conlleva, considerando el principio de mínimo privilegio, es decir, el otorgamiento de acceso mínimo necesario para el cumplimiento de las funciones de su personal.
- Para el establecimiento de acciones de control y responsabilidades en la creación y eliminación de cuentas de acceso de usuarios al ERP SAP se deben seguir las directivas del procedimiento *Control en la Creación y Eliminación de Cuentas de Usuario SAP PROA1-243*. Asimismo, para los sistemas de información diferentes al ERP SAP, estos se adicionarán, de manera gradual, como resultado de lo establecido en el lineamiento *Identificación, Evaluación y Respuesta a los riesgos de Seguridad de la Información – LINA1-025*, complementario al lineamiento *Metodología para identificar, evaluar y dar respuesta a los riesgos corporativos – LINA1-050.*
- Cuando se realice una promoción, reasignación o terminación laboral de los usuarios de la Empresa, sus derechos de acceso

deben ser revisados de acuerdo a las directivas de los procedimientos *Acceso a Facilidades de Cómputo PROA1*-176, y *Control en la Creación y Eliminación de Cuentas de Usuario SAP – PROA1-243.*

- Para solicitar la autorización de derechos de acceso privilegiados, se deben seguir las directivas establecidas en el procedimiento *Acceso a Facilidades de Cómputo PROA1*-176 y lo establecido en el ítem 5.10.5 del presente Reglamento, poniendo énfasis obligatorio en la revisión periódica de dichos usuarios con acceso privilegiados en los recursos de información y Sistema ERP SAP de manera mensual, a fin de verificar la asignación de privilegios o asignación en dichas cuentas, y garantizando que no se asignen sin autorización.

5.10.8. Remoción o ajuste de derechos de acceso (NTP-ISO/IEC 27001-A.9.2.6)

- Para la remoción o ajustes de accesos se debe seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.

5.11. RESPONSABILIDADES DE USUARIOS (NTP-ISO/IEC 27001-A.9.3)

5.11.1. Uso de la información de autenticación secreta (NTP-ISO/IEC 27001-A.9.3.1)

- Para el uso de la información de autenticación secreta, los usuarios deben seguir las directivas del *lineamiento Gestión de Contraseñas – LINA1-086*.

5.12. CONTROL DE ACCESO A SISTEMA Y APLICACIÓN (NTP-ISO/IEC 27001-A.9.4)

5.12.1. Restricción de acceso a la información (NTP-ISO/IEC 27001-A.9.4.1)

- Para solicitar la autorización de derechos de acceso a los recursos de información (entre estos, los sistemas de información) y la información que estas contienen, así como, habilitar los roles o perfiles para controlar el nivel de autorización que se puede tener con el acceso, se deben seguir las directivas establecidas en el procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.
- Los derechos de acceso son independientes entre las aplicaciones, restringiendo de este modo el acceso entre ellas, y para aprobar los accesos los administradores funcionales deben de dar conformidad a las solicitudes.
- Para el sistema ERP-SAP se tiene como control la aplicación de las directivas del procedimiento de *Control en la Creación y Eliminación de Cuentas de Usuario SAP – PROA1-243.*

5.12.2. Procedimientos Seguros de inicio de sesión (NTP-ISO/IEC 27001-A.9.4.2)

- Para el acceso a los sistemas y a las aplicaciones se debe considerar:
  - Emplear una técnica de autentificación, donde se deberían utilizar métodos de autenticación alternativa a las contraseñas, tales como tarjetas inteligentes, token o medios biométricos.
  - No mostrar identificadores de sistemas o aplicaciones hasta que el proceso haya sido completado exitosamente.
  - Mostrar aviso de advertencia que el equipo debería ser accedido solo por usuarios autorizados.
  - No proveer de mensajes de ayuda durante el procedimiento de ingreso que ayudaría a usuarios no autorizados.
  - Validar la información solo cuando se hayan ingresado todos los datos de entrada. Si surge una condición de error, el sistema no debe indicar qué parte de los datos son correctos o incorrectos.
  - Proteger contra intentos de ingreso por fuerza bruta.
  - Registrar intentos fallidos y exitosos.
  - No mostrar la contraseña que está siendo introducida.
  - No transmitir las contraseñas en texto plano (sin cifrar) a través de una red.
  - Ante un posible intento o violación exitosa de ingreso detectado por los controles se debe reportar como un evento de Seguridad.

5.12.3. Sistema de Gestión de Contraseñas (NTP-ISO/IEC 27001-A.9.4.3)

- Para garantizar contraseñas de calidad los sistemas de gestión de contraseñas deben seguir las directivas del *lineamiento Gestión de Contraseñas – LINA1-086*.

5.12.4. Uso de programas utilitarios privilegiados (NTP-ISO/IEC 27001-A.9.4.4)

- El uso de programas utilitarios solamente será autorizado, cuando sea pertinente, por la Gerencia Departamento Tecnologías de Información, para evitar que se instalen programas capaces de anular los controles de los sistemas de información y las aplicaciones.

5.12.5. Control de acceso al código fuente de los programas (NTP-ISO/IEC 27001-A.9.4.5)

- Solo el personal autorizado para la edición y modificación del código fuente tendrá acceso al mismo. La autorización se brindará expresamente siguiendo lo establecido en el procedimiento *Acceso a Facilidades de Cómputo PROA1-176*.
- Se debe implementar un proceso automático o manual que permita controlar el versionamiento del código fuente.

- De ser pertinente establecer en las condiciones de contratación que cualquier código fuente desarrollado por un tercero será de propiedad de PETROPERÚ.

CRIPTOGRAFÍA (NTP-ISO/IEC 27001-A.10)

5.13. CONTROLES CRIPTOGRÁFICOS (NTP-ISO/IEC 27001-A.10.1)

5.13.1. Política sobre el uso de controles criptográficos (NTP-ISO 10.1.1)

- El enfoque de la Dirección respecto a la Seguridad de la Información se encuentra reflejada en los compromisos establecidos en la *Política Corporativa de Seguridad de la Información*, considerando entre estos la confidencialidad e integridad de la información para el empleo de controles criptográficos.
- De acuerdo a lo establecido en el lineamiento *Identificación, Evaluación y Respuesta a los riesgos de Seguridad de la Información – LINA1-025*, complementario al lineamiento *Metodología para identificar, evaluar y dar respuesta a los riesgos corporativos – LINA1-050*, para los resultados de la evaluación de riesgos con niveles o gravedad “Alto” y “Muy Alto”, siempre que sea posible y razonable, se debe aplicar sobre dichos activos de información la implementación de algoritmos con cifrado seguro (considerando tipo, fuerza y calidad) como: AES, RSA, entre otros; según evaluación conjunta de la Jefatura Sistemas Preventivos, y la Gerencia Departamento Tecnologías de Información. La razonabilidad técnica está dada porque efectivamente el control criptográfico ayude a tratar el riesgo asociado al activo en cuestión, de lo contrario el uso de un control de este tipo no sería ni eficaz ni eficiente. Por otro lado, la razonabilidad económica consistirá en verificar que el control criptográfico no cueste más que el beneficio que se obtenga del tratamiento que se le quiera dar al riesgo con el referido control.
- El empleo del cifrado o encriptado seguro, se encuentra implementado para los siguientes dispositivos o servicios:
  - Discos duros de los equipos de trabajo (laptops) proporcionados a los usuarios con la activación de la funcionalidad del “bitlocker” (habilitado para el Sistema Operativo Windows 10 Pro), con un algoritmo de cifrado de XTS-AES (estándar de cifrado avanzado) con fuerza de cifrado de 128 o 256 bits.
  - Para la transferencia de información en servicios de telefonía y videoconferencia.
  - En la conexión remota de los usuarios a la red local mediante acceso VPN (red privada virtual).
- Para gestionar (generación y restauración) las claves o contraseñas de los usuarios, se deben cumplir con las directivas de lo establecido en el *lineamiento Gestión de Contraseñas – LINA1-086*.

En el cifrado de las contraseñas se debe usar algoritmos criptográficos tecnológicamente vigentes y que no presenten expuestos de seguridad.

- Las funciones y responsabilidades de las directivas referidas a criptografía segura deben ser establecidas por la Jefatura Sistemas Preventivos, en coordinación con la Gerencia Departamento Tecnologías de Información, para la ejecución de las mencionadas directivas.

SEGURIDAD FÍSICA Y AMBIENTAL (NTP-ISO/IEC 27001-A.11)

5.14. ÁREAS SEGURAS (NTP-ISO/IEC 27001-A.11.1)

5.14.1. Perímetro de seguridad física (NTP-ISO/IEC 27001-A.11.1.1)

- Para el cumplimiento del presente control respecto a las áreas que contienen información clasificada se debe seguir las directivas del *lineamiento Clasificación de la Información – LA1-GGR-702*.
- Para el cumplimiento del presente control respecto las instalaciones de procesamiento de la información se debe seguir las directivas del *lineamiento Control de Acceso Físico y Protección de Instalaciones de Procesamiento de Datos – LA1-GGR-709*.

5.14.2. Controles de ingreso físico (NTP-ISO/IEC 27001-A.11.1.2)

- Para controlar el ingreso físico al personal de PETROPERÚ se deben seguir las siguientes directivas:
  - ➢ Al ingresar a las instalaciones de PETROPERÚ para el cumplimiento de su jornada laboral, deberá portar su fotocheck personal.
    - ✓ En caso de traer consigo mochilas, maletines deportivos, bolsos, paquetes, estos serán revisados por los agentes de vigilancia.
    - ✓ En caso de no portar su fotocheck personal, deberá solicitar en la recepción de las instalaciones de PETROPERÚ un pase, el cual deberá portar en todo momento y de manera visible, hasta finalizar su jornada laboral.
  - ➢ El uso del fotocheck personal es obligatorio en todo momento y de manera visible.
  - ➢ Si el personal se desplaza entre los ambientes de las Oficinas de Trabajo con su equipo de cómputo, los agentes de vigilancia pueden en cualquier momento solicitar la información del personal o equipo de cómputo que porta.
  - ➢ En caso de percatarse de la presencia de personas extrañas a PETROPERÚ en sus instalaciones, el personal debe consultar el motivo de su visita. De recibir una respuesta inadecuada o una negativa, se debe notificar a los agentes de vigilancia para que tomen las medidas correspondientes.
- Para controlar el ingreso físico de los visitantes se debe seguir las directivas del *Manual Seguridad, Salud y Protección Ambiental para Contratistas – M.SEGU-CO-PR*.

- Para controlar el ingreso físico a las instalaciones de procesamiento de datos se debe seguir las directivas del *lineamiento Control de Acceso Físico y Protección de Instalaciones de Procesamiento de Datos – LA1-GGR-709*.

5.14.3. Seguridad de oficinas, áreas e instalaciones (NTP-ISO/IEC 27001-A.11.1.3)

- Para la seguridad de oficinas, áreas e instalaciones se deben seguir las siguientes directivas:
  - El personal debe portar su fotocheck al ingreso a las instalaciones de PETROPERÚ.
  - En caso de personal sin fotocheck o visitantes, mostrar en los puntos de acceso su DNI (o documento que acredite su identidad) y acercarse al módulo de recepción para cumplir con el procedimiento de acceso.
    - Para controlar el ingreso de los visitantes se debe seguir las directivas del *Manual Corporativo Seguridad, Salud y Protección Ambiental para Contratistas – M.SEGU-CO-PR*.
- Para controlar el ingreso físico a las instalaciones de procesamiento de datos se debe seguir las directivas del *lineamiento Control de Acceso Físico y Protección de Instalaciones de Procesamiento de Datos – LA1-GGR-709*.

5.14.4. Protección contra amenazas externas y ambientales (NTP-ISO/IEC 27001-A.11.1.4)

- Para la protección contra amenazas externas y ambientales se debe seguir las directivas de las siguientes normas:
  - Para el cumplimiento del presente control respecto las instalaciones de procesamiento de la información se debe seguir las directivas del *lineamiento Control de Acceso Físico y Protección de Instalaciones de Procesamiento de Datos – LA1-GGR-709.*
  - Lineamiento *Identificación, Evaluación y Respuesta a los Riesgos de Seguridad de la Información – LINA1-025*.

5.14.5. Trabajo en áreas seguras (NTP-ISO/IEC 27001-A.11.1.5)

- El personal de PETROPERÚ y terceros deben desarrollar sus actividades laborales en los espacios de trabajo y dependencias de la Empresa que le corresponda.
- Para el personal y terceros que realizan sus actividades asignadas en áreas de procesamiento de información de PETROPERÚ, deben seguir las siguientes directivas:
  - En caso que las áreas de procesamiento de información se encuentren desocupadas, estas deben ser cerradas y controladas.
  - Evitar el uso de equipos de fotografía, video, audio u otras formas de registro, salvo autorización expresa de acuerdo al

lineamiento Tomas fotográficas y/o filmaciones de imágenes – LA1-ADM-703.

- Para la realización de trabajos en áreas seguras se debe seguir las directivas del *Manual Corporativo Seguridad, Salud y Protección Ambiental para Contratistas – M.SEGU-CO-PR*.

5.14.6. Zonas de despacho y carga (NTP-ISO/IEC 27001-A.11.1.6)

- Para la seguridad en zonas de despacho y carga en las instalaciones de PETROPERÚ se debe seguir las directivas del *Manual Corporativo Seguridad, Salud y Protección Ambiental para Contratistas – M.SEGU-CO-PR* y del *Reglamento Interno de Seguridad y Salud en el Trabajo*.

5.15. EQUIPOS (NTP-ISO/IEC 27001-A.11.2)

5.15.1. Ubicación y protección de los equipos (NTP-ISO/IEC 27001-A.11.2.1)

- Para la protección de los equipos de cómputo se deben seguir las siguientes directivas:
  - El personal de PETROPERÚ y terceros deben desarrollar sus actividades laborales en los espacios de trabajo y dependencias de la Empresa que le corresponda.
  - El uso del fotocheck personal es obligatorio en todo momento y de manera visible, durante su estancia en PETROPERÚ.
- Para la ubicación, configuraciones (físicas o software) o reparaciones, el personal autorizado para dichas actividades, en cualquiera de las sedes de PETROPERÚ, debe formar parte de la organización de la Gerencia Departamento Tecnologías de Información o de alguno de sus contratistas autorizados para ello.
- Para movimientos de puestos de trabajo de personal con CAP (Cuadro de Asignación Personal), estos deben realizarse con el traslado de equipo de cómputo incluido.
- En caso del personal reasignado a otra dependencia que cuenta con un CAP disponible, este deberá devolver los equipos del puesto anterior y se procederá a asignar equipos de acuerdo al nuevo puesto a ocupar.
- En caso un puesto de trabajo sea removido o fusionado, la dependencia debe devolver los equipos de cómputo asignados a la Gerencia Departamento Tecnologías de Información (Oficina Principal) o Coordinaciones de Servicios TIC de PETROPERÚ.

5.15.2. Servicios de suministro (NTP-ISO/IEC 27001-A.11.2.2)

- Para los servicios de suministro en los centros de procesamiento de información se deben seguir las directivas del *procedimiento Revisión de Requisitos de Seguridad – PA1-GGR-711*, donde se monitorea los servicios de telecomunicaciones, telefonía, UPS, aire acondicionado, entre otros.

- Para los servicios básicos como electricidad, agua, alcantarillado y aire acondicionado, PETROPERÚ debe evaluar la capacidad del crecimiento del negocio, así como realizar las pruebas de inspección regulares para asegurar el buen funcionamiento de dichos servicios, a través de la Dependencia correspondiente de administrar estos servicios.

5.15.3. Seguridad del cableado (NTP-ISO/IEC 27001-A.11.2.3)

- Para la seguridad en el cableado se deben seguir las siguientes directivas:
  - El cableado estructurado utilizado para telecomunicaciones en las instalaciones de PETROPERÚ debe ser de tipo FUTP con categoría 6A (garantizando y asegurando altas tasas de transmisión y evita que se produzca distorsiones).
  - PETROPERÚ debe cumplir con lo señalado en el:
    - ✓ Reglamento Nacional de Edificaciones del Decreto Supremo N° 011-2006-Vivienda, donde se norman los requerimientos para las líneas de energía.
    - ✓ Código Nacional de Electricidad, y modificatorias según Resolución Ministerial N° 175-2008-MEM/DM (Inciso 020-126: Requerimiento Sobre Propagación del Fuego para Alambrado Eléctrico, Conductores y Cables Eléctricos).
  - Para la separación de los cables de energía y de telecomunicaciones para evitar interferencias, utilizar los siguientes los estándares: ANSI/TIA/EIA, ANSI-J-STD, IEEE 802.3an, NTP-ISO/IEC 11801:2002 y IEC-60332-3.
  - Para las instalaciones se deben utilizar tuberías de fierro galvanizado, bandejas metálicas, cajas de paso herméticas y gabinetes (racks) que cumplan los estándares vigentes de cableado estructurado los cuales están situados en ambientes exclusivos, y con acceso solo para personal autorizado.
  - Los paneles de conexión (patcheras) y las salas de cable, se encuentran con ambientes controlados en los cuales los gabinetes (racks) cumplen los estándares vigentes de cableado estructurado, así como con llaves físicas que solo son manejadas por personal autorizado.

5.15.4. Mantenimiento de equipos (NTP-ISO/IEC 27001-A.11.2.4)

- Para el mantenimiento de los equipos de cómputo se deben seguir las directivas del *procedimiento Mantenimiento Correctivo de Equipos de Cómputo Propiedad de PETROPERÚ – PA0-GGR-713*.
- Para el mantenimiento de los equipos TIC, las acciones deben considerar las recomendaciones del fabricante, lugar de instalación y el tiempo de uso del equipo al momento de realizarse el mantenimiento. Esta actividad debe ser realizada anualmente, previa planificación del Contratista autorizado para ello y aprobación de PETROPERÚ.

- El personal autorizado para realizar el mantenimiento de los equipos es el Contratista Autorizado para ello, previa coordinación y aprobación de la Gerencia Departamento Tecnologías de Información.

5.15.5. Retiro de activos (NTP-ISO/IEC 27001-A.11.2.5)

- Para el retiro de los equipos se debe seguir las directivas de los *procedimientos Autorización para Uso de Equipos de Cómputo de PETROPERÚ fuera de las Instalaciones – PA1-GGR-705* e *Ingreso, salida y uso de equipo de cómputo particular – PA1-GGR-706*.
- Para movimientos de puestos de trabajo de personal con CAP (Cuadro de Asignación Personal), estos deben realizarse con el traslado de equipo de cómputo incluido.
- En caso un puesto de trabajo sea removido o fusionado, la dependencia debe devolver los equipos de cómputo asignados a la Gerencia Departamento Tecnologías de Información (Oficina Principal).

5.15.6. Seguridad de equipos y activos fuera de las instalaciones (NTP-ISO/IEC 27001-A.11.2.6)

- Para el retiro de los equipos se debe seguir las directivas de los *procedimientos Autorización para Uso de Equipos de Cómputo de PETROPERÚ fuera de las Instalaciones – PA1-GGR-705* e *Ingreso, Salida y Uso de Equipo de Cómputo Particular – PA1-GGR-706*.
- Para dispositivos móviles (como USB, discos externos, CD, DVD) que contengan información digital, y para información impresa que sea detectada por los agentes de vigilancia durante el retiro del personal debe ser registrado el nombre del personal, ficha, código del dispositivo, e información que está siendo retirada (Información Impresa) para su posterior reporte a la dependencia del personal que retira el dispositivo.

5.15.7. Eliminación segura o reúso de equipos (NTP-ISO/IEC 27001-A.11.2.7)

- Para la eliminación segura o reúso de equipos, se deben seguir las siguientes directivas:
  - Para la instalación y el retiro de los equipos de cómputo, por motivo de obsolescencia o reemplazo implica que la Gerencia Departamento Tecnologías de Información debe proceder con el borrado físico y lógico de la información almacenada en dichos equipos de cómputo, a través de una herramienta informática especializada para tal fin.
  - Para puestos de trabajo que sean removidos o fusionados, la dependencia debe devolver los equipos de cómputo asignados a la Gerencia Departamento Tecnologías de Información (Oficina Principal) o Coordinaciones de Servicios TIC de PETROPERÚ.

- Para la disposición final de los residuos de aparatos eléctricos y electrónicos (RAEE) se deben seguir las directivas del *procedimiento Gestión y Manejo de Residuos de aparatos Eléctricos y Electrónicos (RAEE) – PA1-DES-013.*

5.15.8. Equipos de usuario desatendidos (NTP-ISO/IEC 27001-A.11.2.8)

- Al dejar un equipo desatendido temporalmente, el usuario debe bloquear el acceso a su estación de trabajo, independientemente del tiempo que permanezcan alejados.
- Al terminar la jornada de trabajo se debe apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina y respondan a labores propias del cargo del usuario.
- Se debe cerrar la sesión de administrador de los equipos de cómputo, cuando el usuario con dicho rol ha concluido su labor.
- Para el caso de los dispositivos móviles “laptops”, éstos deben ser guardados en gabinetes o cajonerías bajo llave.
  El protector de pantalla debe activarse automáticamente a los quince (15) minutos de estar desatendida la estación de trabajo.

5.15.9. Política de escritorio y pantalla limpia (NTP-ISO/IEC 27001-A.11.2.9)

- Al finalizar la jornada laboral, los usuarios no deben dejar papeles de trabajo con información confidencial sobre sus escritorios. Asimismo, no deben dejar medios magnéticos u ópticos con información de la organización. El almacenamiento de estos elementos se debe realizar en gabinetes o cajonería bajo llave.
- La información clasificada como confidencial del negocio debe custodiarse en ambientes controlados que garanticen su seguridad.
- Los usuarios deben autorizar y supervisar el uso de su equipo de trabajo, cuando el personal de Mesa de Ayuda acceda local o remotamente al equipo.
- Los usuarios deben evitar guardar archivos confidenciales, con los que trabajen, en el escritorio de sus equipos de cómputo.
- Se debe tener especial cuidado con el uso de dispositivos como fotocopiadoras o impresoras de manera que el material con información confidencial no permanezca en ellas sin atención.
- No se debe utilizar papel reciclado que contenga información confidencial.

SEGURIDAD DE LAS OPERACIONES (NTP-ISO/IEC 27001-A.12)

5.16. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES (NTP-ISO/IEC 27001-A.12.1)

5.16.1. Procedimientos operativos documentados (NTP-ISO/IEC 27001-A.12.1.1)

- La creación o actualización, registro, aprobación, publicación y caducidad de los procedimientos o lineamientos operativos, debe realizarse de acuerdo a lo establecido en el *lineamiento Gestión de Documentos Normativos – LINA1-030.*
- Los documentos normativos deben elaborarse teniendo en cuenta el *lineamiento Elaboración de Documentos Normativos – LINA1-031* y *el formato de Elaboración de Documentos Normativos – FORA1-300 v.0*.
- Seguir las instrucciones operativas incluidas en los siguientes documentos:
  - *Lineamiento Gestión de Correo Electrónico – LA1-ADM-716 (establece criterios para: solicitud de creación de cuenta de correo, denominación de la cuenta, acceso a los servicios de correo, capacidad de mensajes).*
  - *Procedimiento Autorización para Uso de Equipos de Cómputo de PETROPERÚ Fuera de las Instalaciones – PA1-GGR-705 y Procedimiento Ingreso, Salida y Uso de Equipo de Cómputo Particular – PA1-GGR-706 (especifican instrucciones para manipulación de salidas y medios especiales).*
  - *Procedimiento Gestión de Incidentes de Seguridad de la Información PA1-GGR-704 (especifica instrucciones para el manejo de errores u otras condiciones excepcionales).*
  - *Procedimiento Revisión de Requisitos de Seguridad – PA1-GGR-711 (establece criterios para las verificaciones seguridad física de los centros de cómputo)*
  - *Procedimiento Mantenimiento Correctivo de Equipos de Cómputo Propiedad de PETROPERÚ – PA0-GGR-713.*
- Además, se deben elaborar procedimientos o lineamientos con instrucciones operativas, entre otros aspectos, sobre lo siguiente:
  - *Reinicio y recuperación de sistemas de información ante la ocurrencia de fallas o incidentes.*
  - *Gestión de registros de eventos de actividades en los sistemas de información.*
  - *Copias de respaldo de seguridad de la información, software y sistemas.*

5.16.2. Gestión del cambio (NTP-ISO/IEC 27001-A.12.1.2)

- Para la gestión de cambio se deben seguir las siguientes directivas:
  - Identificar y registrar los cambios significativos.
  - Realizar controladamente, y en forma oportuna y planificada los cambios en los componentes de Tecnologías de Información administrados.

- Minimizar los incidentes como resultado de la introducción de cambios al entorno de Tecnologías de Información administrado.
- Mantener el balance entre las necesidades del negocio para innovar y la necesidad de mantener el servicio de Tecnologías de Información.
- Para casos donde se tenga que atender una necesidad de negocio urgente, restaurar la disponibilidad de un servicio, o resolver un incidente de forma temporal o definitiva, se deben coordinar "cambios de emergencia".

5.16.3. Gestión de la capacidad (NTP-ISO/IEC 27001-A.12.1.3)

- Para la gestión de la capacidad se deben seguir las siguientes directivas:
  - Identificar y entender el rendimiento, capacidad y utilización de cada uno de los componentes individuales dentro de la tecnología utilizada para brindar soporte.
  - Definir los umbrales de capacidad referidos a los servidores que soportan los servicios.
  - Generar y mantener un plan de capacidad.
  - Garantizar que los logros de rendimiento, cumplan los objetivos de rendimiento acordados.
  - Colaborar con el diagnóstico, y resolución de incidencias y problemas, asociados con la capacidad.
  - Evaluar el impacto de todos los cambios en el plan de capacidad.
  - Asegurar que se implementen medidas proactivas para mejorar el rendimiento de los servicios.

5.16.4. Separación de los entornos de desarrollo, pruebas y operaciones (NTP-ISO/IEC 27001-A.12.1.4)

- Para la separación de entornos de desarrollo, pruebas y operaciones (producción) se deben seguir las siguientes directivas:
  - Definir las reglas para la transferencia de los paquetes de software entre los entornos.
  - Probar los cambios en los sistemas y aplicaciones en el entorno de pruebas antes de ser aplicados en el entorno de operaciones (producción).
  - Evitar realizar pruebas directamente en el entorno de operaciones (producción), salvo casos excepcionales debidamente autorizados por el Comité de Cambios.
  - Evitar instalar software utilitario en el entorno de operaciones (producción), salvo casos excepcionales debidamente autorizados por el Comité de Cambios.
  - Los entornos deben emplear perfiles de usuarios diferentes para los sistemas y aplicaciones.

- La información clasificada como confidencial no debería copiarse en el entorno de pruebas, a menos que se enmascare la información.

5.17. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS (NTP-ISO/IEC 27001-A.12.2)

5.17.1. Controles contra códigos maliciosos (NTP-ISO/IEC 27001-A.12.2.1)

- Para el control contra códigos maliciosos se debe seguir las directivas del lineamiento *Protección Contra Código Malicioso – LINA1-058*, *procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704, lineamiento LA1-GGR-715 Formulación del Programa de Capacitación de Seguridad de la Información* (que incluye actividades de capacitación, concientización y difusión quincenal de tips de Seguridad de la Información), y las Circulares GTIC-017-2012, GADM-004-2007 y GSIN-038-2007, que regulan el uso de software y prohíben la instalación no autorizada del mismo.

5.18. COPIA (NTP-ISO/IEC 27001-A.12.3)

5.18.1. Respaldo de la información (NTP-ISO/IEC 27001-A.12.3.1)

- Para el respaldo de la información se deben seguir las siguientes directivas:
  - Establecer un modelo reusable y escalable de soluciones de respaldo de la información y recuperación de datos, independiente de herramientas y productos específicos, sin perder de vista los factores técnicos y de negocios.
  - Describir las actividades de respaldo y recuperación de la información.
  - Crear, mantener y ejecutar el plan de respaldo y recuperación de la información.
  - Probar los planes de respaldo de la información y procedimientos derivados correspondientes.

5.19. REGISTROS Y MONITOREO (NTP-ISO/IEC 27001-A.12.4)

5.19.1. Registro de eventos (NTP-ISO/IEC 27001-A.12.4.1)

- La bitácora de eventos que registran las actividades de los sistemas de información (ERP SAP y no SAP) y dispositivos, deben considerar, siempre que sea técnicamente posible, lo siguiente:
  - Identificador (ID) de usuario.
  - Actividades del sistema.
  - Fechas, horarios y detalles de los eventos clave como: inicio y cierre de sesión.
  - Identificador (ID) y ubicación del dispositivo.
  - Registros de acceso a los sistemas exitosos y rechazados, así como a los datos y otros intentos de acceso a los recursos.
  - Registros en cambios de la configuración de los sistemas.
  - Registros en el uso de privilegios.

- Registro de archivos accedidos y tipos de accesos.
- Definir alarmas planteadas por el sistema de control de accesos.
- Para los dispositivos de seguridad perimetral, se deben registrar la activación y desactivación de los sistemas de protección.
- Registro de transacciones realizadas por los usuarios en los sistemas de información.

- La obtención de los registros de eventos se realiza de forma manual para su análisis según requerimiento, asimismo, para el desarrollo consistente del mantenimiento y revisión de dichos registros de eventos se requiere de una herramienta automatizada (SIEM – Gestión de Información y Eventos de Seguridad, o Correlacionador de Eventos). El alcance de los sistemas de información y dispositivos serán definidos de acuerdo con el lineamiento *Identificación, Evaluación y Respuesta a los riesgos de Seguridad de la Información – LINA1-025*, complementario al lineamiento *Metodología para identificar, evaluar y dar respuesta a los riesgos corporativos – LINA1-050,* identificando a los activos de información que comprometan riesgos con niveles o gravedad “Alto” y “Muy Alto”.

5.19.2. Protección de información de registros (NTP-ISO/IEC 27001-A.12.4.2)

- Los medios de registros deben contar con una adecuada gestión de accesos para sus usuarios, a fin de evitar cambios no autorizados, alteración o eliminación de la información de registros.
- La información de registros (logs) tiene un periodo de almacenamiento en los servidores de seis (6) meses a partir de su generación (elaboración), pasado dicho periodo se realizan copias de respaldo (backups) de la información de registros que serán almacenadas por un periodo de un (1) año.

5.19.3. Registros de administrador y operador (NTP-ISO/IEC 27001-A.12.4.3)

- Para los usuarios con acceso administrador u operador (cuentas privilegiadas) de los sistemas de información o aplicaciones, se deben registrar sus eventos de acuerdo a las directivas establecidas en el control 5.19.1. del presente Reglamento de Seguridad de la Información.
- Asimismo, los usuarios con acceso administrador u operador, siempre que sea técnicamente posible, no deben contar con permisos de manipular (modificar o eliminar) los registros de sus eventos realizados.

5.19.4. Sincronización de reloj (NTP-ISO/IEC 27001-A.12.4.4)

- Los relojes de todos los sistemas de procesamiento de la información de PETROPERÚ deben estar sincronizados al servidor de tiempo ntp.petroperu.com.pe, sincronizado con un servidor de tiempos de Stratum-2; por lo que es un nivel de referencia válido.

5.20. CONTROL DE SOFTWARE OPERACIONAL (NTP-ISO/IEC 27001-A.12.5)

5.20.1. Instalación de software en sistemas operacionales (NTP-ISO/IEC 27001-A.12.5.1)

- Para la instalación de software en sistemas operacionales se deben seguir las siguientes directivas:
  - La Gerencia Departamento Tecnologías de Información debe evaluar el impacto y urgencia de todas las solicitudes de pases a producción recibidas, en base a su experiencia sobre el negocio para evaluar la aprobación de los pases solicitados.
  - Mantener el balance entre las necesidades del negocio para innovar y la necesidad de mantener el servicio de Tecnologías de Información.

5.21. GESTIÓN DE VULNERABILIDAD TÉCNICA (NTP-ISO/IEC 27001-A.12.6)

5.21.1. Gestión de vulnerabilidades técnicas (NTP-ISO/IEC 27001-A.12.6.1)

- Para la gestión de vulnerabilidades técnicas se deben seguir las siguientes directivas:
  - En los contratos con proveedores que involucren desarrollo de aplicaciones o sistemas web que se encontrarán publicadas en la red informática de PETROPERÚ, deben considerarse requerimientos de evaluación de vulnerabilidades técnicas para mitigar los riesgos que puedan existir con el producto antes de su pase a producción.
  - La Gerencia Auditoría Interna y Riesgos en coordinación con la Gerencia Departamento Tecnologías de Información, anualmente ejecuta el servicio de ethical hacking para los dispositivos y aplicaciones críticas en la red interna y externa informática de PETROPERÚ.

5.21.2. Restricciones sobre la instalación de software (NTP-ISO/IEC 27001-A.12.6.2)

- Para las restricciones sobre la instalación de software en los equipos de cómputo y dispositivos móviles de PETROPERU, se deben seguir las siguientes directivas:
  - Los usuarios de la red informática de PETROPERÚ no cuentan con el privilegio de administrador de los equipos de cómputo o dispositivos móviles proporcionados por la Empresa, por lo tanto, no pueden instalar ningún tipo de software.
  - En caso de los usuarios con privilegios de administrador, estos no deben realizar ninguna instalación de software sin la debida

autorización de su dependencia y la Gerencia Departamento Tecnologías de Información.

- De igual manera, considerar las directivas de las Circulares GTIC-017-2012, GADM-004-2007 y GSIN-038-2007, que regulan el uso de software y prohíben la instalación no autorizada del mismo.

5.22. CONSIDERACIONES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN (NTP-ISO/IEC 27001-A.12.7)

5.22.1. Controles de auditoría de sistemas de información (NTP-ISO/IEC 27001-A.12.7.1)

- Para los requisitos y actividades de auditoria de sistemas de información, se deben seguir las siguientes directivas:
  - Acordar y coordinar los requisitos de auditoría de acceso a los sistemas e información.
  - Acordar y controlar el alcance de las verificaciones de auditoría.
  - Las verificaciones deberían limitarse a solo permisos de lectura al software e información.
  - En caso sea necesario y debidamente evaluado, permitir copias aisladas de archivos del sistema que deben ser borradas una vez completada la auditoría o mantenidas con los controles de seguridad adecuados.

SEGURIDAD DE LAS COMUNICACIONES (NTP-ISO/IEC 27001-A.13)

5.23. GESTIÓN DE SEGURIDAD DE LA RED (NTP-ISO/IEC 27001-A.13.1)

5.23.1. Controles de la red (NTP-ISO/IEC 27001-A.13.1.1)

- Para el acceso de los usuarios a la red Corporativa de PETROPERÚ, se deben seguir las directivas del procedimiento *Acceso a Facilidades de Cómputo PROA1-176,* caso contrario dicho acceso es restringido.
- Para la conexión de los usuarios a la red Corporativa de PETROPERÚ (física e inalámbrica), la autenticación se realiza a través de la dirección MAC (Media Access Control) de su equipo de cómputo asignado y las credenciales del usuario (nombre de usuario y contraseña) para dicho equipo existente en el directorio activo, validado con el software de servicio de identidad.
- La conexión para usuarios que tienen acceso VPN (red privada virtual) cuenta con protocolos de seguridad como SSL e IPSEC, evitando de este modo intentos de robo o interceptación de la información.
- La Gerencia Departamento Tecnologías de Información es responsable del mantenimiento y soporte de la LAN (red de área local) y WAN (red de área amplia) informática de PETROPERÚ.

5.23.2. Seguridad de servicios de red (NTP-ISO/IEC 27001-A.13.1.2)

- La Gerencia Departamento Tecnologías de Información es responsable del monitoreo sobre la red corporativa informática de PETROPERÚ.
- La Gerencia Departamento Tecnologías de Información debe establecer acuerdos de seguridad para sus servicios de red administrados, asegurando su implementación.
- La asignación de direcciones IP (Internet Protocol) para los equipos y dispositivos que se encuentran conectados a la red informática Corporativa de PETROPERÚ, deben ser realizados de manera dinámica y asignados por dominios (zonas) de cada operación.
- Las peticiones de acceso a los servicios de la red informática interna Corporativa de PETROPERÚ deben ser solicitadas desde equipos y dispositivos ubicados dentro de la red Corporativa, en caso que las peticiones sean solicitadas externamente a la red Corporativa no deben brindar respuesta.
- Se debe deshabilitar los accesos a los servicios de red que no sean utilizados.

5.23.3. Segregación en redes (NTP-ISO/IEC 27001-A.13.1.3)

- La red informática Corporativa de PETROPERÚ debe estar debidamente segmentada, a fin de facilitar su gestión y no comprometer la disponibilidad de sus servicios. Las redes de las sedes de PETROPERÚ deben estar segmentadas de la siguiente manera:
  - Para edificios se tienen VLAN's (red de área local virtual) por cada piso.
  - Para sedes sin edificios, se encuentran las VLAN's distribuidas por áreas o dependencias organizacionales.

5.24. TRANSFERENCIA DE INFORMACIÓN (NTP-ISO/IEC 27001-A.13.2)

5.24.1. Políticas y procedimientos de transferencia de información (NTP-ISO/IEC 27001-A.13.2.1)

- Para la transferencia de información en servicios de telefonía y videoconferencia se debe contar con protocolos de comunicación seguros (como TLS o SRTP) que permitan mantener la confidencialidad, integridad y autenticidad de la información.
- Las VPN (redes privadas virtuales) deben contar con protocolos de seguridad como SSL e IPSEC, evitando de este modo intentos de robo o interceptación.

5.24.2. Acuerdos sobre transferencia de información (NTP-ISO/IEC 27001-A.13.2.2)

- Para los acuerdos de transferencia de información se deben seguir las siguientes directivas:

- Clasificar la información de acuerdo al *lineamiento Clasificación de la Información – LA1-GGR-702*, para su respectivo etiquetado.
- Todas las dependencias que entreguen información a organizaciones externas a PETROPERÚ deben incluir acuerdos de custodia.
- Procedimientos para asegurar la trazabilidad y el no repudio (negación) de la información.

- Las responsabilidades y compromisos en el caso de incidentes de seguridad de la información, deben seguir las directivas del *procedimiento Gestión de Incidentes de Seguridad de la Información PA1-GGR-704.*
- Las responsabilidades de la transferencia de la información por la entrega ante la culminación de una contratación de servicios que comprometían procesamiento de información, deben estar debidamente definidas en las cláusulas de los contratos celebrados con los proveedores o terceros, así como la forma y medios de entrega de la información, y las condiciones que deben cumplir ambas partes ante la resolución del vínculo.

5.24.3. Mensajería electrónica (NTP-ISO/IEC 27001-A.13.2.3)

- El acceso a redes sociales debe ser asignado a personal que para el desarrollo de sus funciones en la Empresa deba contar con dichos privilegios, por ejemplo, Gerencia Departamento Comunicaciones, Gerencia Departamento Marketing, entre otros.
- La mensajería electrónica relacionada a temas de la Empresa debe realizarse a través de equipos de cómputo o dispositivos móviles asignados por la Empresa.
- Adicionalmente, se deben seguir las directivas del *lineamiento Gestión de Correo Electrónico – LA1-ADM-716*.

5.24.4. Acuerdos de confidencialidad o no divulgación (NTP-ISO/IEC 27001-A.13.2.4)

- Para acuerdos de confidencialidad o de no divulgación, se deben seguir las directivas de los procedimientos:
  - *Contrataciones del Personal (Anexo 4 – Declaraciones Juradas Contratación de Personal) – PROA1-072.*
  - *Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710.*
- La duración de los acuerdos de confidencialidad o no divulgación deben tener una temporalidad mínima de cinco (05) años para terceros a partir de terminado su contrato y para el personal desvinculado de la Empresa. El propietario de la Información debe evaluar la temporalidad de la Confidencialidad, terminado el Servicio.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN (NTP-ISO/IEC 27001-A.14)

5.25. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (NTP-ISO/IEC 27001-A.14.1)

5.25.1. Análisis y especificaciones de requisitos de Seguridad de la Información (NTP-ISO/IEC 27001-A.14.1.1)

- Dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes, se deben especificar los controles o requerimientos de seguridad asociados; los cuales deben considerar lo siguiente:
  - Requisitos de autenticación del usuario, por ejemplo, uso de contraseña, Captcha, autenticación de dos fases.
  - Gestión de acceso y de procesos de autorización.
  - Registros de Auditoría, según criticidad del dato o transacción.
  - Las necesidades de protección requeridas de los activos involucrados, en particular en relación con la disponibilidad, la confidencialidad y la integridad.
  - Cifrar el canal de comunicación entre todas las partes implicadas.

5.25.2. Aseguramiento de los servicios de aplicaciones sobre redes públicas (NTP-ISO/IEC 27001-A.14.1.2)

- Para los servicios de aplicación que pasan a través de las redes públicas se debe considerar:
  - Evaluación y definición del nivel de confianza requerido por cada parte participante.
  - Procesos de autorización asociados con quién puede emitir o aprobar el contenido de los documentos transaccionales clave;
  - Que los usuarios de aplicaciones son plenamente informados de sus autorizaciones para la prestación o uso del servicio.
  - La prevención de la pérdida o duplicación de la información de la transacción;
  - La responsabilidad asociada con cualquier transacción fraudulenta.
- Los acuerdos de servicios de aplicaciones que establezca PETROPERÚ con terceros deben estar respaldados por un acuerdo documentado que compromete a ambas partes a los términos acordados de servicios, incluyendo los detalles de la autorización.

5.25.3. Protección de las transacciones en servicios de aplicaciones (NTP-ISO/IEC 27001-A.14.1.3)

- Las consideraciones de seguridad de la información para transacciones de servicios de aplicación deben incluir lo siguiente:
  - Garantizar los aspectos de toda transacción: validar y verificar la información secreta de autenticación y conservar la privacidad asociada con todas las partes implicadas.

- Cifrar el canal de comunicación entre todas las partes implicadas.
- Almacenar los detalles de la transacción, en un ambiente protegido.
- Incorporar la seguridad en todo el proceso de Gestión del certificado o firma digital.

5.26. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE (NTP-ISO/IEC 27001-A.14.2)

5.26.1. Política de desarrollo seguro (NTP-ISO/IEC 27001-A.14.2.1)

Los lineamientos, procedimientos y estándares para el desarrollo de software y sistemas, deben considerar lo siguiente:

- Requerimientos y controles de seguridad:
  - Control de autenticación: creación de usuarios con contraseñas robustas.
  - Control de roles y privilegios: cada usuario debe tener acceso a lo necesario dentro de la aplicación.
- En la fase de análisis y diseño considerar el modelado de amenazas, para lo cual se debe realizar:
  - Diseño seguro de mensajes de errores: no se debe mostrar información en los mensajes de error, que pudieran dar pistas sobre el acceso a la aplicación.
  - Diseño seguro para evitar SQL INJECTION.
  - Diseño de autenticación y login.
- Durante la codificación:
  - Validar los datos de entrada antes de procesarlos, para evitar ataques por SQL INJECTION.
  - Controlar el tamaño y el tipo de datos de entrada, para evitar riesgos en la entrada de datos en los formularios.
  - Evitar mezclar datos con código fuente (Hard – code).
  - Evitar el uso de sentencias SQL dinámicas, priorizando el uso STORED PROCEDURES (Procedimientos almacenados).
  - Análisis de código fuente.
- Realizar un Análisis de vulnerabilidades a las aplicaciones que pasarán a Producción. y subsanar las vulnerabilidades identificadas, realizando finalmente una configuración de seguridad.

5.26.2. Procedimientos de control de cambio del sistema (NTP-ISO/IEC 27001-A.14.2.2)

- Para el control de cambios se debe seguir las directivas del Procedimiento “Gestión de Requerimientos” – PROA1-168 y “Control de Requerimientos” - PROA1-089.
- La introducción de nuevos sistemas y cambios importantes a sistemas existentes, debe seguir un proceso formal de documentación, especificación, pruebas, control de calidad, implantación (Pase a producción) y gestión de la implementación.

Este proceso deberá incluir una evaluación de riesgos, el análisis de los impactos de los cambios y especificación de controles necesarios, entre los que se pueden considerar:

- Asegurar que los cambios son efectuados por personas autorizadas.
- Revisar y asegurar que los controles ya implementados no se comprometan por los cambios.
- Identificar la aplicación, información, base de datos y hardware que requiera enmiendas.
- Identificar y controlar el código crítico para reducir al mínimo la probabilidad de fallos de seguridad.
- Al terminar cada cambio la documentación del sistema debe ser actualizada y la documentación anterior, archivada.
- Manejar un sistema de control de versiones.
- Manejar trazabilidad de todos los cambios solicitados.
- Según sea necesario, actualizar los procedimientos o manuales de usuarios.
- Realizar el pase a producción en el momento adecuado, donde no se interfiera con los procesos de negocio implicados.

Las actualizaciones automatizadas no deben utilizarse sobre los sistemas críticos.

5.26.3. Revisión técnica de aplicaciones después de cambios a la plataforma operativa (NTP-ISO/IEC 27001-A.14.2.3)

- Antes de efectuar los cambios en las aplicaciones, se debe elaborar y ejecutar casos de pruebas. Así también, las aplicaciones impactadas deberán ser verificadas una vez realizados los cambios en los ambientes de producción.
- Para las aplicaciones que lo requieran, ejecutar las Pruebas Especiales (entre las que encontramos Pruebas de Estrés, Performance y Análisis de vulnerabilidades). Y efectuar las correcciones que sean pertinentes.

5.26.4. Restricciones sobre cambios a los paquetes de software (NTP-ISO/IEC 27001-A.14.2.4)

- En la medida de lo posible, los paquetes de software, suministrados por contratistas, deberían utilizarse sin modificaciones.
- Cuando un paquete de software necesite ser modificado se debe:
  - Identificar los riesgos de comprometer los procesos de control e integridad existentes.
  - Obtener el consentimiento del fabricante del software, considerando la garantía si se realiza las modificaciones.
  - Evaluar la posibilidad de que el contratista que provee el software, que debe estar debidamente autorizado por el Fabricante para efectuar este tipo de actividades, realice las modificaciones como actualizaciones normales del programa.
  - Evaluar y comunicar a la dependencia interesada en la modificación si, como consecuencia del cambio, la Empresa

debe hacerse cargo del futuro mantenimiento. Si se persiste en la modificación del paquete, la dependencia interesada en la modificación, deberá asumir el riesgo y el impacto que la modificación genere.

5.26.5. Principios de ingeniería de sistemas seguros (NTP-ISO/IEC 27001-A.14.2.5)

- Diseñar la seguridad en todas las capas de arquitectura (Negocios, Datos, Aplicaciones y Tecnologías) equilibrando la necesidad de Seguridad de la Información con la necesidad de Accesibilidad.
- Se deben establecer procedimientos y lineamientos de desarrollo seguro de las aplicaciones en los que se incorporen técnicas de autenticación, control seguro de sesiones, validación de datos.

5.26.6. Ambiente de desarrollo seguro (NTP-ISO/IEC 27001-A.14.2.6)

- Establecer ambientes de desarrollo seguros, considerando:
  - Evaluar la sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema.
  - Cumplir los requisitos externos e internos aplicables (Política, Reglamento, Procedimientos, entre otros).
  - Considerar los controles de seguridad existentes en la Organización.
  - Evaluar al personal que trabaja en el entorno.
  - Separar los diferentes entornos de desarrollo.
  - Gestionar los accesos al entorno de desarrollo.
  - Los respaldos deben ser almacenados en locaciones fuera de las instalaciones.

5.26.7. Desarrollo contratado externamente (NTP-ISO/IEC 27001-A.14.2.7)

- Cuando el desarrollo del sistema es contratado con un tercero, considerar:
  - Los acuerdos de licencias, propiedad del código, y derechos de propiedad intelectual relacionados con el contenido de terceros.
  - Cumplimiento de las Políticas, Procedimientos y lineamientos de Desarrollo Seguro de PETROPERÚ.
  - Pruebas de aceptación y verificación de calidad de los entregables.
  - Pruebas para protegerse contra la presencia de contenido malicioso intencional y no intencional en la entrega.
  - Pruebas de Escaneo de vulnerabilidades conocidas.
  - Derecho contractual de auditar a los procesos y a los controles de desarrollo.

5.26.8. Pruebas de seguridad del sistema (NTP-ISO/IEC 27001-A.14.2.8)

- Realizar pruebas de los sistemas nuevos y actualizados durante el proceso de Desarrollo.
- Los equipos de desarrollo deben incluir pruebas internas.
- Deben realizarse pruebas de aceptación independiente del equipo desarrollador.
- La extensión de las pruebas debe ser proporcional a la naturaleza y criticidad del Sistema.

5.26.9. Pruebas de aceptación del sistema (NTP-ISO/IEC 27001-A.14.2.9)

- Las pruebas de aceptación del Sistema siempre deben incluir las pruebas de los requisitos de Seguridad de la Información.
- Las pruebas de aceptación deben realizarse en ambiente de pruebas independiente del ambiente de producción; los cuales deben tener las mismas condiciones.
- Las pruebas deben ser llevadas a cabo tanto en los componentes recibidos como en los sistemas integrados.
- Realizar el escaneo de vulnerabilidades, a los sistemas que lo ameriten, y realizar las correcciones.
- Cuando se requiera, coordinar con la Jefatura Sistemas Preventivos, la realización de escaneo de vulnerabilidades de los sistemas en la red externa, a través del servicio contratado para tal fin.

5.27. DATOS DE PRUEBAS (NTP-ISO/IEC 27001-A.14.3)

5.27.1. Protección de datos de prueba (NTP-ISO/IEC 27001-A.14.3.1)

- Cuando los datos de producción son usados para realizar pruebas, para proteger estos datos se deben seguir las siguientes directivas:
  - El control de accesos, que se aplica a sistemas de aplicaciones en producción debe aplicarse también a los sistemas de pruebas.
  - Cada vez que se requiera copiar información de producción a un ambiente de prueba debe autorizarse, por los niveles correspondientes.
  - Evaluar la necesidad de enmascarar los datos según sea requerido. Si se utiliza información personal o cualquier otra información sensible para hacer pruebas, todos los detalles y contenido sensible deben eliminarse o en su defecto enmascararse.

RELACIÓN CON CONTRATISTAS (NTP-ISO/IEC 27001-A.15)

5.28. SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS CONTRATISTAS (NTP-ISO/IEC 27001-A.15.1)

5.28.1. Política de Seguridad de la Información para las relaciones con los contratistas (NTP-ISO/IEC 27001-A.15.1.1)

- Para la Seguridad de la Información en las relaciones con los contratistas se debe seguir las directivas del *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710, así como, lo especificado en el Anexo 2 del Presente Reglamento, referente a contratos con Terceros.*

5.28.2. Abordar la seguridad dentro de acuerdos con contratistas (NTP-ISO/IEC 27001-A.15.1.2)

- Para abordar la seguridad dentro de acuerdos con los contratistas se debe seguir las directivas pertinentes del *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710*, *así como, lo especificado en el Anexo 2 del Presente Reglamento referente a contratos con Terceros.*

5.28.3. Cadena de suministro de tecnología de información y comunicaciones (NTP-ISO/IEC 27001-A.15.1.3)

- Para abordar la seguridad en la cadena de suministro de tecnología de información y comunicaciones se debe seguir las directivas pertinentes del *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710*.

5.29. GESTIÓN DE ENTREGA DE SERVICIOS DEL CONTRATISTA (NTP-ISO/IEC 27001-A.15.2)

5.29.1. Monitoreo y revisión de servicios de los contratistas (NTP-ISO/IEC 27001-A.15.2.1)

- Para los servicios con contratistas que manejen activos de información de PETROPERÚ, las Unidades responsables de administrar los contratos de los servicios deben comunicar la ocurrencia de fallas e incidentes de acuerdo al *procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704*.

5.29.2. Gestión de cambios de los servicios del contratista (NTP-ISO/IEC 27001-A.15.2.2)

- Para la gestión de cambio de los servicios de los contratistas se debe seguir las directivas pertinentes del *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros - PA1-GGR-710, así como, lo especificado en el Anexo 2 del Presente Reglamento referente a contratos con Terceros.*

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (NTP-ISO/IEC 27001-A.16)

5.30. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS (NTP-ISO/IEC 27001-A.16.1)

5.30.1. Responsabilidades y procedimientos (NTP-ISO/IEC 27001-A.16.1.1)

- Las responsabilidades de la gestión de incidentes de Seguridad de la Información se establecen en el *procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704*.

5.30.2. Reporte de eventos de Seguridad de la Información (NTP-ISO/IEC 27001-A.16.1.2)

- Los reportes de eventos de Seguridad de la Información se canalizan a través del correo electrónico de la Jefatura Sistemas Preventivos (sistemaspreventivos@petroperu.com.pe), según lo establecido en el *procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704*.
- Adicionalmente, los incidentes de Seguridad de la Información relacionados con Tecnologías de la Información, también son canalizados a través de la Mesa de Ayuda de Tecnologías de la Información (Anexo 77777).

5.30.3. Reporte de debilidades de Seguridad de la Información (NTP-ISO/IEC 27001-A.16.1.3)

- Los usuarios y terceros deben identificar y reportar cualquier debilidad de Seguridad de la Información observada o sospechada, a su jefatura inmediata o al administrador del contrato, quienes deberán tomar las medidas correctivas que se ameriten y notificar a la Jefatura Sistemas Preventivos, o Gerencia Departamento Tecnologías de Información.
- Los usuarios y terceros no deben probar si pueden vulnerar sistemas aprovechando presuntas debilidades de Seguridad de la Información.

5.30.4. Evaluación y decisión sobre los eventos de Seguridad de la Información (NTP-ISO/IEC 27001-A.16.1.4)

- Se debe evaluar el evento y determinar si este puede ser clasificado dentro de cualquiera de los criterios de Clasificación para incidentes. Si el evento configura un incidente de Seguridad de la Información, debe registrarse e informarse al Usuario que reportó el evento.
- Si se requiere la participación de algún especialista, para investigar y determinar las acciones de solución pertinentes, se debe registrar; y el Oficial SI debe comunicarle su participación, vía correo electrónico, con copia a su Jefe inmediato superior.

5.30.5. Respuesta a incidentes de Seguridad de la Información (NTP-ISO/IEC 27001-A.16.1.5)

- Para dar respuesta a los incidentes de Seguridad de la Información se deben seguir las directivas especificadas en el *procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704*.

5.30.6. Aprendizaje de los incidentes de Seguridad de la Información (NTP-ISO/IEC 27001-A.16.1.6)

- Los resultados de la investigación y solución de los incidentes de Seguridad de la Información deben utilizarse para:
  - Reducir la probabilidad o impacto de futuros incidentes similares.
  - Retroalimentar y fortalecer el proceso de gestión de incidentes.
  - Identificar incidentes recurrentes o de alto impacto.
  - Sensibilizar y capacitar a los usuarios y terceros.

5.30.7. Recolección de evidencia (NTP-ISO/IEC 27001-A.16.1.7)

- Durante el proceso de investigación y determinación de las causas y consecuencias del incidente, el *Supervisor Sistemas Preventivos* y los especialistas convocados para la investigación del incidente, deben recolectar y registrar las evidencias, relacionadas con el incidente.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (NTP-ISO/IEC 27001-A.17)

5.31. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN (NTP-ISO/IEC 27001-A.17.1)

Al no existir un sistema de gestión de continuidad del negocio (SGCN) formal, ni planificación de recuperación de desastres (DRP), se asume que los requisitos de Seguridad de la Información siguen siendo los mismos en situaciones adversas en comparación con las condiciones de funcionamiento normales.

5.31.1. Planificación de continuidad de Seguridad de la Información (NTP-ISO/IEC 27001-A.17.1.1)

- Para la planificación de continuidad de Seguridad de la Información en situaciones adversas, se debe desarrollar un análisis de impacto del negocio (BIA) a nivel de procesos, a fin de determinar los requisitos de seguridad de la información aplicables en estas situaciones.

5.31.2. Implementación de continuidad de Seguridad de la Información (NTP-ISO/IEC 27001-A.17.1.2)

- Para la implementación de continuidad de Seguridad de la Información en situaciones adversas, PETROPERÚ debe asegurarse de:
  - Establecer una estructura de gestión adecuada, a fin de preparar, mitigar y responder a un evento disruptivo, utilizando personal con autoridad, experiencia y competente.
  - Designar personal de respuesta a incidentes de seguridad de la información de acuerdo al procedimiento Gestión de Incidentes de Seguridad de la Información – PA1-GGR-704.
  - Desarrollar y aprobar planes documentados para gestionar un evento disruptivo y mantener su seguridad de la información en los niveles alineados en la planificación.
- Asimismo, PETROPERÚ debe establecer, documentar, implementar y mantener los:
  - Controles de seguridad de la información dentro de los procesos, procedimientos y sistemas a apoyo.
  - Procesos y procedimientos para el mantenimiento de controles de seguridad de la información ante una situación adversa.
  - Controles compensatorios para los controles de seguridad de la información que no pueden ser mantenidos en una situación adversa.

5.31.3. Verificación, revisión y evaluación de continuidad de Seguridad de la Información (NTP-ISO/IEC 27001-A.17.1.3)

- Para la verificación, revisión y evaluación de la gestión de la continuidad de Seguridad de la Información en situaciones adversas, PETROPERÚ debe:
  - Ejercitar y probar las funcionalidades de los procesos, procedimientos y controles de continuidad de la seguridad de la información.
  - Ejercitar y probar el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de seguridad de la información.
  - Revisar la validez y eficacia de las medidas de continuidad de la seguridad de la información ante algún cambio de los sistemas de información, procesos, procedimiento y controles de seguridad de la información.

5.32. REDUNDANCIAS (NTP-ISO/IEC 27001-A.17.2)

5.32.1. Instalaciones de procesamiento de la información (NTP-ISO/IEC 27001-A.17.2.1)

- Para el cumplimiento de la disponibilidad de las instalaciones (centros) de procesamiento de la información, se deben seguir las siguientes directivas:
  - En caso de indisponibilidad en la instalación de procesamiento de información de la Oficina Principal (OFP), se habilitará como

centro de procesamiento de información las operaciones Talara o Conchán.

- Los controles ambientales de los centros de procesamiento de información de PETROPERÚ, cuentan con su respectiva redundancia por cada tipo, como: aniego, aire acondicionado, sistema de alimentación de energía ininterrumpida (UPS) y sistemas contra incendios (FM-200).

- Para el monitoreo de las instalaciones de procesamiento de la información, PETROPERÚ debe considerar lo siguiente:
  - Para los servicios críticos, validar el informe mensual que emite el proveedor de servicios de tecnología y comunicaciones, relacionado a los controles que aseguren la redundancia en las condiciones ambientales y dispositivos tecnológicos. Así como, coordinar con el proveedor de servicios de tecnología y comunicaciones, una visita anual a fin de validar sus controles ambientales y tecnológicos que garanticen la continuidad de las operaciones.

CUMPLIMIENTO (NTP-ISO/IEC 27001-A.18)

5.33. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES (NTP-ISO/IEC 27001-A.18.1)

5.33.1. Identificación de requisitos contractuales y de legislación aplicables (NTP-ISO/IEC 27001-A.18.1.1)

- Gerencia Legal, Gerencia Departamento Tecnologías de Información, y Gerencia Auditoría Interna y Riesgos, deben revisar continuamente la publicación de los dispositivos legales, a fin de identificar, documentar y mantener los aplicables a Seguridad de la Información.

5.33.2. Derechos de propiedad intelectual (NTP-ISO/IEC 27001-A.18.1.2)

- Para el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual, se debe seguir las directivas pertinentes del *procedimiento Tratamiento de Riesgos Relacionados a Contratos con Terceros – PA1-GGR-710*.

5.33.3. Protección de registros (NTP-ISO/IEC 27001-A.18.1.3)

- Para el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a la protección de registros, se debe seguir las directivas pertinentes del procedimiento Retención y Eliminación de Registros de Información – PA1-GGR-712.

5.33.4. Privacidad y protección de datos personales (NTP-ISO/IEC 27001-A.18.1.4)

- Para asegurar la privacidad y protección de datos personales, PETROPERÚ debe cumplir con la:

- Política Corporativa de Protección de Datos Personales de PETROPERÚ.
- Ley N° 29733 – Ley de Protección de Datos Personales.
- Lineamiento *Privacidad de Datos Personales – LINA1–062*.
- Procedimiento *Atención de derechos de acceso, rectificación, cancelación y oposición (ARCO) – PROA1–285*.

5.33.5. Regulación de controles criptográficos (NTP-ISO/IEC 27001-A.18.1.5)

- Gerencia Legal, Gerencia Departamento Tecnologías de Información, y Gerencia Auditoría Interna y Riesgos, deben evaluar continuamente la pertinencia de establecer normas relacionadas a controles criptográficos en la Empresa.

5.34. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN (NTP-ISO/IEC 27001-A.18.2)

5.34.1. Revisión independiente de la Seguridad de la Información (NTP-ISO/IEC 27001-A.18.2.1)

- Para la revisión independiente de la Seguridad de la Información, la Gerencia Auditoría Interna y Riesgos debe programar y gestionar dicha revisión por personas independientes a la Dependencia en evaluación.
- La revisión debe realizarse cada dos (2) años y debe definirse el alcance de la evaluación.

5.34.2. Cumplimiento de políticas y normas de seguridad (NTP-ISO/IEC 27001-A.18.2.2)

- Las Gerencias y Gerencias Departamento deben revisar regularmente el cumplimiento de las políticas y normas de Seguridad de la Información, a fin de detectar incumplimiento y evaluar la necesidad de tomar medidas correctivas.

5.34.3. Revisión de cumplimiento técnico (NTP-ISO/IEC 27001-A.18.2.3)

- Para la revisión del cumplimiento técnico, la Jefatura Sistemas Preventivos, tiene como responsabilidad gestionar el servicio de Ethical Hacking anualmente.

VI. RECOMENDACIONES O PRECISIONES

PRIMERA: Aplicación Supletoria
Para lo no previsto expresamente en el presente reglamento, se aplicará lo dispuesto en el Estatuto Social o norma aplicable a PETROPERÚ.

SEGUNDA: Vigencia y gradualidad de implementación
El presente reglamento entrará en vigencia a partir de su publicación en la Intranet Corporativa.

Si como parte de la entrada en vigencia del Reglamento, fuera necesario implementar nuevos controles o mejorar los existentes, éstos serán implementados durante el proceso de implementación del SGSI en el que se realizará el registro, documentación, elaboración y aplicación de los controles requeridos por la NTP-ISO/IEC 27001, aplicable a todas las instalaciones de la Empresa, que incluye las redes IT (Information Technology), OT (Operational Technology) y otros.

La Alta Dirección proporcionará los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua de los controles necesarios para el buen desempeño de la Gestión de la Seguridad de la Información y cumplimiento del presente Reglamento.

TERCERA: Difusión y Supervisión del Reglamento

La difusión a todos los usuarios, estará a cargo de Gerencia General, Gerencias Nivel 2, Gerencias Departamento, Jefes y Supervisores, en forma de cascada.
La Jefatura Sistemas Preventivos 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 todos los usuarios, a través de la Gerencia Gestión de Personas.

Gerencia Legal, Gerencia Departamento Tecnologías de Información, y Gerencia Auditoría Interna y Riesgos, deben evaluar continuamente la pertinencia del establecimiento de nuevas normas aplicables al presente Reglamento.

CUARTA: Incumplimiento del Reglamento

Los incumplimientos del presente Reglamento que originen perjuicio a la Empresa darán lugar a la apertura de un proceso de investigación, a fin de determinar las acciones que sean pertinentes.

QUINTA: Normativa Vigente

Cuando se haga referencia a normativa (Políticas, Lineamientos, Procedimientos e Instructivos) en el presente Reglamento, se refiere a la normativa vigente.
La normativa interna referenciada (Políticas, Lineamientos, Procedimientos e Instructivos) en este Reglamento es la que se encuentra vigente.
En caso se realice una actualización a la normativa, esta debe ser informada a la Jefatura Sistemas Preventivos, para la revisión y evaluación de la actualización del presente Reglamento.

SEXTA: Controles no considerados

El presente Reglamento no considera los siguientes controles:

- A.10.1.2: Gestión de claves, se implementarán a medida de su desarrollo tecnológico en la Empresa.

SÉTIMA: Aprobación

El presente reglamento reemplaza su versión anterior "REGA1-004 Reglamento de Seguridad de la Información v.2", aprobado por Gerencia General el 30.01.2019, por encargo del Presidente del Directorio, según lo señalado en el Acuerdo de Directorio N° 100-2017-PP del 25.11.2017.

La actualización del presente Reglamento de Seguridad de la Información ha sido propuesta por el Comité de Seguridad de la Información, integrado según lo dispuesto en la Hoja de Acción N° GGRL-0235-2021, para aprobación de Gerencia General.
Fecha de próxima actualización: 15.07.2023.
Responsable de próxima revisión: Jefatura Sistemas Preventivos.

VII. CAMBIOS CON RESPECTO A LA VERSIÓN ANTERIOR

- Este documento actualiza y deja sin vigencia el reglamento REGA1-004 v.2 “Reglamento de Seguridad de la Información”.
- Los cambios corresponden a la actualización de los siguientes ítems de los controles alineados a las especificaciones de la ISO/IEC 27002:2013. Tecnología de la Información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la Información:
  - 5.3.1 Política de dispositivos móviles, correspondiente al control NTP-ISO/IEC 27001-A.6.2.1.
  - 5.3.2 Teletrabajo, correspondiente al control NTP-ISO/IEC 27001-A.6.2.2.
  - 5.10.7 Revisión de derechos de acceso de usuarios, correspondiente al control NTP-ISO/IEC 27001-A.9.2.5.
  - 5.12.1 Restricción de acceso a la información, correspondiente al control NTP-ISO/IEC 27001-A.9.4.1.
  - 5.13.1 Política sobre uso de controles criptográficos, correspondiente al control NTP-ISO/IEC 27001-A.10.1.1.
  - 5.19.1 Registro de eventos, correspondiente al control NTP-ISO/IEC 27001-A.12.4.1.
  - 5.19.3 Registros del administrados y del operador, correspondiente al control NTP-ISO/IEC 27001-A.12.4.3.
- Asimismo, se han actualizado las referencias de la normativa interna de PETROPERÚ a lo largo del presente Reglamento.

VIII. PROCESO AL QUE PERTENECE

Código del Proceso	Nombre del Proceso	Nivel del Proceso
D2.4	Sistemas Preventivos	1

IX. ANEXOS

ANEXO 1: Glosario de Términos
ANEXO 2: Requisitos de Seguridad de la Información con Empleados, Colaboradores, Usuarios y Otros Terceros

Fecha:

ANEXO 1: Glosario de Términos

1. **Activo de Información:**
   Recurso del sistema de información o relacionado con éste, necesario para que la organización alcance los objetivos propuestos.
2. **Ambiente o Área Controlada:**
   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.
3. **Análisis de Impacto del Negocio (BIA):**
   Proceso de análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (NTP-ISO/IEC 22301:2019)
4. **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 realizan las actividades de identificación, evaluación, y tratamiento de los riesgos, que permiten construir un registro histórico de los 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.
5. **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 el usuario es quien dice ser.
6. **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 la Dependencia donde presta servicio. Los autorizados a formular dicha solicitud, están establecidos en el Cuadro de Niveles de Autoridad y Responsabilidad.
7. **Códigos Ocultos Maliciosos o Código Troyano:**
   Es un programa computacional que aparentemente es útil, pero ejecutan programas ocultos que causan daños; estos códigos pueden encontrarse en las aplicaciones software no autorizados.
8. **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.
9. **Control:**
   Política, reglamento, procedimientos, lineamientos, prácticas 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.
10. **Control por Oposición:**
    Se establece para mantener una adecuada segregación de funciones sobre una tarea o actividad, de tal forma que un usuario o una Dependencia de la

organización pueda iniciar y registrar las transacciones mientras un segundo usuario o Dependencia de la gestión lo revisa de manera concurrente.

11. **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.
12. **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.
13. **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 "PETROPERÚ.com.pe".
14. **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 desencriptar o descifrar la información nuevamente.
15. **Customisar:**
    Es 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.
16. **Empleado:**
    Toda persona natural que presta servicios en PETROPERÚ, con contrato de trabajo a plazo indeterminado, plazo fijo o cualquier otra modalidad de contrato de trabajo.
17. **Equipo Informático:**
    Aquel bien que almacena, traslada y procesa información, sean estos propios o contratados bajo cualquier modalidad por PETROPERÚ.
18. **Estación de Trabajo:**
    Es el equipo, computadora personal o portátil, asignada al usuario de PETROPERÚ, conforme a los procedimientos derivados de la Política Corporativa y Reglamento de Seguridad de la Información.
19. **Herramientas de Ofimática:**
    Son aquellas que 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, entre otros.

- Programas de e-mail, correo de voz, mensajeros, dispositivos inalámbricos.
- Suite o paquete ofimático: paquete de múltiples herramientas ofimáticas como Microsoft Office, Open Office, entre otros.

20. **Información Confidencial (Restringida, Uso Interno) / Pública:**
Toda información es Pública con excepción de lo señalado en la Ley de Transparencia y Accesos a la Información.
21. **Interfaz Gráfica:**
Conocida como GUI, por sus siglas en inglés: Graphical User Interface, 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 qué hora ocurrieron, así como referencias a dichas fallas, entre otros.
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. **OT (Operational Technology):**
Es el hardware y software dedicado a detectar o causar cambios en los procesos físicos a través del monitoreo y / o control directo de dispositivos físicos como válvulas, bombas, etc.

27. **Propietario de Activo de Información**:
Son los Gerentes Nivel 2, Gerentes Departamento, Jefes o 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.
28. **Propietario del Riesgo**
Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.

29. **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.
30. **Red de Datos (Information Technology: IT):**
    Consiste en la interconexión entre las estaciones de trabajo con que cuenta PETROPERÚ. La Red de Datos incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.
31. **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.
32. **Retención de Registros:**
    Intervalo de tiempo que almacenamos un registro antes de eliminarlo.
33. **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.
34. **Seguridad Informática:**
    Son las técnicas desarrolladas para proteger los equipos informáticos o sistemas conectados en una red, frente a daños accidentales o intencionados.
35. **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.
36. **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.
37. **Sistema de Detección de Intrusos (IDS):**
    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).
38. **Soporte Técnico:**
    Es el servicio de asesoría, mantenimiento y reparación que brinda la Gerencia Departamento Tecnologías de Información a los usuarios de PETROPERÚ, en forma presencial o remota, mediante comunicaciones telefónicas, por correo electrónico o por cualquier otro medio de comunicación interna.
39. **Tratamiento de Información:**
    Es una serie ordenada de operaciones realizadas sobre la información: captación, almacenamiento, clasificación, elaboración y utilización de la información.
40. **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 Nivel 2, Gerentes Departamento, Jefes, Supervisores, Trabajadores o Empleados, Practicantes, Consultores,

Prestadores de Servicios Profesionales, Personal de Empresas Contratistas, entre otros.

41. 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.

Fecha:

ANEXO 2: Requisitos de Seguridad de la Información con Empleados, Colaboradores, Usuarios y Otros Terceros

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, Manual, Reglamento, Procedimientos y Lineamientos 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 detectadas en los mismos a la Dependencia de Sistemas e Informática, y a la Jefatura Sistemas Preventivos, es considerado un incumplimiento de la Política Corporativa, Reglamento, Procedimientos y Lineamientos 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 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, Manual, Reglamento, Procedimientos y Lineamientos 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 detectadas en los mismos a la Dependencia de Sistemas e Informática, y a la Jefatura Sistemas Preventivos, es considerado un incumplimiento de la Política Corporativa, Reglamento, Procedimientos y Lineamientos de Seguridad de la Información de PETROPERÚ".

- **Contratos con Terceros:**

  "El contratista deberá cumplir con la Política Corporativa, Manual, Reglamento, Procedimientos y Lineamientos 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".

"No mantener el riguroso cuidado de los activos de información de PETROPERÚ otorgados para su uso, ni avisar a tiempo de fallas detectadas en los mismos a las Dependencias de Sistemas e Informática, y a la Jefatura Sistemas Preventivos, es considerado un incumplimiento de la Política Corporativa, Reglamento, Procedimientos y Lineamientos 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, Manual, Reglamento de Seguridad de la Información, cuando sean de aplicación.

En caso que se requiera realizar un cambio o precisión a las cláusulas antes descritas, se requiere el visto bueno de la Jefatura Sistemas Preventivos, y la aprobación de la Gerencia Legal.

Fecha: