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

- La Sub Gerencia Sistemas e Informática es responsable del monitoreo sobre la red corporativa informática de PETROPERÚ.
- La Sub Gerencia Sistemas e Informática 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:

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

- 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.*

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, la Sub Gerencia Comunicaciones, la Sub Gerencia 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:
  - *Contratación de Personal (Anexo 5 – Declaración jurada para ingreso del 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)

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

- 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.

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

- 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

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

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

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

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, etc).
  - 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.

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

- 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 Unidad Sistema de Control Interno y Seguridad de la Información, 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 directrices:
  - 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.

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

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.*

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

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 Unidad Sistema Control Interno y Seguridad de la Información (usi@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 7777).

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 Unidad Sistema Control Interno y Seguridad de la Información, o Sub Gerencia Sistemas e Informática.
- 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

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

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 *Analista de Control Interno y Seguridad de la Información* 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)

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

- 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 directrices:
  - En caso de indisponibilidad en la instalación de procesamiento de información de la Oficina Principal (OFP),

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

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)

- La Gerencia Corporativa Legal, la Sub Gerencia Sistemas e Informática, y la Sub Gerencia Control Interno y Gestión de 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.

Revisión 1	Revisión 2	Revisión 3	Aprobado
CAROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS SUAREZ PILO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 35863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	Fecha: 30.01.2019 ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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

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.

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

- La Gerencia Corporativa Legal, la Sub Gerencia Sistemas e Informática, y la Sub Gerencia Control Interno y Gestión de 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 Sub Gerencia Control Interno y Gestión de 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 Sub Gerencias 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 Unidad Sistema Control Interno y Seguridad de la Información, 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.

Revisión 1	Revisión 2	Revisión 3	Aprobado
			Fecha: 30.01.2019

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

NIOLA PALACIOS TOLEDO
Sub Gerente
Control Interno y Gestión de Riesgos
Ficha: 55221

LUIS CARLO
Gerente
Corporativo Planeamiento
Gestión y Riesgos
Ficha: 33863

CARLOS Y. LINARES PEÑALOZA
Gerente (e) Corporativo Finanzas
Ficha: 57980

ESTEBAN BERTARELLI B.
Gerente General
Ficha: 54087

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, Sub Gerencias, Jefes y Supervisores, en forma de cascada.
La Unidad Sistema Control Interno y Seguridad de la Información promoverá la adecuada difusión del contenido y alcances del Reglamento, así como la supervisión de su estricto cumplimiento, para lo cual deberá orientar la capacitación a todos los usuarios, a través de la Gerencia Corporativa Recursos Humanos.

La Gerencia Corporativa Legal, la Sub Gerencia Sistemas e Informática, y la Sub Gerencia Control Interno y Gestión de 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 Unidad Sistema de Control Interno y Seguridad de la Información, para la revisión y evaluación de la actualización del presente Reglamento.

Revisión 1	Revisión 2	Revisión 3	Aprobado
CAROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS ALBERTO CARLO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 35863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	Fecha: 30.01.2019 ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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

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 desarrollando tecnológico en la Empresa.
- A.6.2.2: Teletrabajo, su desarrollo será gradual a medida que la Empresa implemente sus directivas.

SÉTIMA: Aprobación

El presente reglamento reemplaza su versión anterior "MASI-002 Reglamento de Seguridad de la Información v.1.", aprobado con Acuerdo de Directorio N° 032-2013-PP del 18.04.2013. Con Acuerdo de Directorio N° 100-2017-PP del 25.11.2017, se encargó a Gerencia General la aprobación de la actualización del Reglamento de Seguridad de la Información de PETROPERÚ S.A, alineado a la Política Corporativa de Seguridad de la Información y a la Norma Técnica Peruana vigente.

La actualización de este 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° GCPL-SCGR-001-2017, para aprobación de Gerencia General.

Fecha de próxima actualización: 31.12.2020.

Responsable: Unidad Sistema Control Interno y Seguridad de la Información.

VII. CAMBIOS CON RESPECTO A LA VERSIÓN ANTERIOR

Los cambios corresponden al cumplimiento de la Resolución Ministerial N° 004-2016-PCM, donde se aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos; dejando sin efecto a su versión anterior basada en la Política Corporativa de Seguridad de la Información y la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.

VIII. PROCESO AL QUE PERTENECE

Código del Proceso	Nombre del Proceso	Nivel del Proceso
S6.3	Sistema de Gestión de Seguridad de la Información	1

IX. ANEXOS

ANEXO 1: Glosario de Términos

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

Revisión 1	Revisión 2	Revisión 3	Aprobado
CAROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS EDUARDO CARLO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 33863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	Fecha: 30.01.2019 ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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

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 22301:2012)
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.

Revisión 1	Revisión 2	Revisión 3	Aprobado
CAROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS LÓPEZ CARLO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 35863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	Fecha: 30.01.2019 ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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

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.

Revisión 1	Revisión 2	Revisión 3	Aprobado
			Fecha: 30.01.2019
ROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS FUENTES CARLO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 33863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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

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, Sub Gerentes, 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 Sub Gerencia Sistemas e Informática.
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 Sub Gerencia Sistemas e Informática a los usuarios de PETROPERÚ, en forma

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

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, Sub Gerentes, 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.

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 Unidad Sistemas de Control Interno y Seguridad de la Información, 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 Unidad Sistemas de Control Interno y Seguridad de la Información, es considerado un incumplimiento de la Política Corporativa, Reglamento, Procedimientos y Lineamientos de Seguridad de la Información de PETROPERÚ".

ESTE DOCUMENTO HA SIDO PREPARADO PARA USO EXCLUSIVO DE PETROPERÚ
No debe ser reproducido sin autorización expresa 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 Unidad Sistemas de Control Interno y Seguridad de la Información, 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 Unidad Sistema de Control Interno y Seguridad de la Información, y la aprobación de la Gerencia Corporativa Legal.

Revisión 1	Revisión 2	Revisión 3	Aprobado
CAROLA PALACIOS TOLEDO Sub Gerente Control Interno y Gestión de Riesgos Ficha: 55221	LUIS E. LINARES CARLO Gerente Corporativo Planeamiento Gestión y Riesgos Ficha: 35863	CARLOS A. LINARES PEÑALOZA Gerente (e) Corporativo Finanzas Ficha: 57980	Fecha: 30.01.2019 ESTEBAN BERTARELLI B. Gerente General Ficha: 54087

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