HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Cambios realizados en el documento
1	Enero -2016	Emisión de la primera versión del documento. Resolución No. 2016004.
2	Mayo-2018	Revisión anual de la Política de Seguridad de la Información Institucional y actualización del código del documento de PCA.16. DR.01 por PCA.01.02. DR.01. Acta No. 00481.
3	Octubre-2020	Revisión anual de la Política de Seguridad de la Información Institucional. Acta No. 00691.
4	Octubre-2022	Revisión anual de la Política de Seguridad de la Información Institucional. Se incluye los Lineamientos 4.6 y 4.7, se modifica el punto 5.6. Cambio de código de PCA.01.02.DR.01 a PCA.04.01.DR.01.
5	Agosto - 2023	Revisión anual de la Política de Seguridad de la Información Institucional. Actualización de formato. Se modifica en el numeral 4.1 del apartado Lineamientos considerando la serie de normas 27000 y no únicamente 27001.
6	Mayo - 2024	Revisión anual de la Política de Seguridad de la Información Institucional. Actualización integral del documento en función del Acuerdo Ministerial 2024-0003 - EGSI v3.
7	Junio - 2025	Revisión anual de la Política de Seguridad de la Información Empresarial, aprobada por el Comité de Seguridad de la Información en sesión de 15 de mayo de 2025, conforme se evidencia del Acta de la Segunda Reunión Ordinaria (2025). Se modifica el Punto dos “Alcance” por “Ámbito de Aplicación”. Se incluye el Punto 4 “Principios de Seguridad de la Información” y se modifica la numeración de todo el documento a partir de dicho punto. Se incluye en el punto 6 “Definición de términos” los conceptos de “Información”, “Seguridad de la Información” y se modifica el concepto de “Propietario de información” Se incluyen las reglas 7.30 hasta la 7.33 Se modifican las reglas 8.19, 8.20, 8.21 y 8.23 del apartado “Subgerencia de Tecnologías de la Información y Comunicaciones”. Se incluye la regla 8.29 en el apartado Subgerencia de Logística y Abastecimiento Se modifica el apartado “Subgerencia de Planificación y Control de Gestión” por “Jefatura de Seguridad y Transparencia de la Información”, de este apartado se modifican las reglas 8.37, 8.38, 8.39, 8.40, 8.41 y se incluye la regla 8.43. Se incluye la regla 8.49 del apartado “Jefatura de PMO Empresarial” Se eliminan las reglas 7.46 y 7.47 del apartado “Oficial de Seguridad de la Información” y se modifica las reglas 8.50 y 8.52 Se incluye el apartado 9. Cumplimiento de Normativa. En todo el documento se modifica la frase “Comité de Seguridad y Trasparencia de la Información” por “Comité de Seguridad de la Información”.

1. Introducción

La Empresa Pública de Hidrocarburos del Ecuador EP PETROECUADOR, reconoce a la información como un activo indispensable para el cumplimiento de su misión, visión y objetivos empresariales, por lo tanto, debe ser protegida a fin de preservar la confidencialidad, integridad y disponibilidad de la misma a través de un Sistema de Gestión de Seguridad de la información (SGSI).

2. Ámbito de aplicación

La *"Política de Seguridad de la Información Empresarial"* es un eje transversal de cumplimiento y aplicación obligatoria en los procesos de la Empresa, para todo el personal de la EP PETROECUADOR y agentes externos que intervienen en el ciclo de vida de la información (generar, almacenar, usar, compartir, archivar y eliminar) tanto en medios físicos como digitales.

3. Objetivo

Establecer y adoptar directrices para una adecuada gestión de la seguridad de la información en la empresa con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información física y digital mediante la implementación de controles preventivos, de detección y correctivos alineados al cumplimiento de los objetivos empresariales.

4. Principios de Seguridad de la Información

- Confidencialidad: La información debe ser accesible solo a las personas autorizadas y con una necesidad legítima de conocerla.
- Integridad: La información debe mantenerse precisa, completa y actualizada, evitando alteraciones no autorizadas.
- Disponibilidad: La información debe estar disponible para los usuarios autorizados cuando sea necesario para su operación y toma de decisiones.
- Cumplimiento Legal: La empresa cumplirá con la legislación ecuatoriana sobre protección de datos personales, derechos de propiedad intelectual y demás normativas relacionadas con la seguridad de la información.
- Defensa en profundidad: La empresa identificará los activos críticos y adoptará un enfoque mediante múltiples capas de seguridad para garantizar un análisis exhaustivo y la detección de posibles intrusiones.

5. Compromiso

La Gerencia General, reconoce a la información empresarial como un activo clave para el cumplimiento de los objetivos estratégicos empresariales, por lo que mantiene el compromiso de cumplir y hacer cumplir los principios de confidencialidad, integridad y disponibilidad de la información observando en todo momento las leyes, políticas y normativa vigente, mediante la implementación y mejora continua del Sistema de Seguridad de la Información (SGSI) empresarial.

6. Definición de Términos

Activo de información. - Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Amenaza. - Causa potencial de un incidente no deseado, que puede provocar daños en un sistema u organización.
Ataque. - Intento no autorizado, con o sin éxito, de destruir, alterar, inutilizar o acceder a un activo o cualquier intento de exponer, robar o hacer un uso no autorizado de un activo.
Confidencialidad. - Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Disociación. - Procedimiento que consiste en modificar la información para que no se pueda identificar a una persona. Un dato disociado es aquel que no permite la identificación de su titular de forma directa ni indirecta.
Disponibilidad. - Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma cuando éstos lo requieran.
Enmascaramiento. - Es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacenamiento, cambiando su información, pero consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida**.**
Información: Es uno de los activos más importantes para la empresa, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.
Incidente de seguridad de la información. - Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad. - Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
Interrupción. - Incidente, previsto o imprevisto, que provoca una desviación negativa y no planificada de la entrega prevista de productos y servicios de acuerdo con los objetivos de una organización.
Privacidad. - Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.
Propietario de Información. - Es la máxima autoridad de cada área administrativa u operativa, dueño del proceso donde se genera o crea activos de información, trabajadores que por un rol asignado (por ejemplo: administradores de contrato, presidentes o secretarios de comités, etc.) tengan la responsabilidad de gestionar el acceso a información de acuerdo al ámbito de sus competencias. El propietario del activo de información es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
Registro. - Información creada, recibida y conservada como prueba y como un activo por una organización o persona, en cumplimiento de obligaciones legales o en la transacción de negocios.
Riesgo. - Combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la Información. - Es la preservación de la confidencialidad, integridad, disponibilidad, autenticidad, y no repudio mediante un conjunto de medidas preventivas y reactivas sobre los activos de información en el marco de la gestión pública, a fin de garantizar la protección de la información crítica y el cumplimiento de las leyes, normativas y regulaciones aplicables a las entidades del sector público.
Sistema de información. - Conjunto de aplicaciones, servicios, activos de tecnologías de la información u otros componentes que manejan información.
Usuarios externos. - Persona o entidad fuera de EP Petroecuador que requiere acceso a información empresarial. Por ejemplo, proveedores.
Vulnerabilidad. - Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. Lineamientos generales

7.1. Las disposiciones previstas en este documento son de aplicación obligatoria para todo el personal de la EP PETROECUADOR y usuarios externos, en la ejecución de los procesos empresariales o prestación del servicio que corresponda a nivel nacional.

7.2. La EP PETROECUADOR minimizará la ocurrencia e impacto de los eventos que ponen en riesgo la seguridad de la información, a través de la implementación del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27000, otros instrumentos establecidos en la normativa legal vigente dispuestos por entes de control; y, mediante procesos, procedimientos, documentos relacionados o cualquier otra normativa interna de la EP PETROECUADOR.

7.3. La EP PETROECUADOR realizará la valoración del riesgo de los activos de información para contemplar acciones y controlar las situaciones de riesgo a fin de minimizar el impacto en los objetivos empresariales, según las responsabilidades establecidas en el Reglamento del Comité de Seguridad de la Información.

7.4. Los controles de seguridad a implementar se determinan por el resultado del análisis de riesgo; o por el cumplimiento de requisitos legales, estatutarios, y por principios, objetivos estratégicos y necesidades de la EP PETROECUADOR, para dar soporte a sus operaciones.

7.5. Toda operación y transacción con la información de la empresa deberá disponer de la debida autorización y aprobación de la autoridad competente, cumpliendo las condiciones determinadas en la normativa legal aplicable.

7.6. Los requerimientos de información de la ciudadanía en general deberán seguir los procedimientos vigentes de entrega de información a terceros según lo definido en el Proceso de Gestión Documental o al Proceso de Gestión de la Transparencia de la Información (PCA.05) según corresponda.

7.7. La información confidencial o reservada que sea entregada por parte de las diferentes unidades orgánicas y de negocio de la EP PETROECUADOR a otras instituciones del Estado o entidades externas debe estar regulada por los respectivos instrumentos legales de intercambio de información, acuerdos de reserva y confidencialidad de información que se suscriban para el efecto.

7.8. La entrega de información digital o física, clasificada como confidencial, deberá realizarse mediante la suscripción del Acuerdo de Confidencialidad con Terceros, a excepción de los requerimientos efectuados por autoridades administrativas, legislativas o judiciales. En caso de ser necesario, este tipo de requerimientos deberán atenderse sometiendo la información a procedimientos de anonimización, seudonimización, cifrado, enmascaramiento de datos u otras técnicas de protección.

7.9. La entrega y recepción de información reservada o confidencial no podrá realizarse por correo electrónico, mensajería instantánea, o redes sociales. Para este fin, únicamente deberá hacerse uso de medios de transmisión de información seguros y establecidos por la empresa.

7.10. Las transacciones y operaciones ejecutadas como parte de los procesos de la empresa deben mantener registros de la trazabilidad de las distintas unidades orgánicas y de negocio, y funcionarios involucrados a lo largo del proceso.

7.11. Se clasificará y protegerá los activos de información empresarial, implementando las medidas de seguridad que correspondan según el caso, tomando en cuenta los controles establecidos en las mejores prácticas o normativa vigente.

7.12. Todo medio que contenga, almacene o custodie información confidencial o reservada en formato físico o digital, de acuerdo con el inventario de activos de la información aprobado, obligatoriamente debe estar protegido y respaldado según las medidas empresariales definidas para dicho efecto.

7.13. La información empresarial se debe clasificar en función de los requisitos legales determinados por los entes de control, el nivel de sensibilidad, criticidad y susceptibilidad

a divulgación o modificación no autorizada. Los niveles estarán determinados en el proceso de Gestión de Seguridad de la Información. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades judiciales, legislativas u órganos de control competentes, o en caso de violación a los derechos humanos.

7.14. La EP Petroecuador realizará un programa de concientización a los trabajadores, pasantes, proveedores y contratistas sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades laborales, mediante planes de comunicación y capacitación continua.

7.15. La EP PETROECUADOR considerará la seguridad informática como un mecanismo de protección para la información, que permita controlar o evitar las amenazas cibernéticas, las cuales ponen en riesgo la información que es procesada, transmitida y almacenada por medios digitales.

7.16. Toda la información creada, almacenada y procesada en los computadores de escritorio y/o portátiles asignados al personal de la institución, así como los recursos tecnológicos asignados al personal, son de propiedad de la EP PETROECUADOR, motivo por el cual, conforme al proceso Gestión de la Seguridad de la Información, se podrá realizar el monitoreo y control aplicando el procedimiento de evaluación correspondiente.

7.17. La gestión de proyectos de la empresa debe integrar durante todo el ciclo de vida del proyecto, el análisis de riesgos de seguridad de la información a fin de que se identifiquen, evalúen y traten de forma temprana considerando las medidas aplicables, independientemente del tipo de proyecto a desarrollar.

7.18. Todos los funcionarios de la empresa y usuarios externos que usan los servicios y sistemas de información de la institución, deben informar cualquier debilidad de seguridad, evento o incidentes de la información observada o sospechada en los sistemas o servicios de la empresa al Oficial de Seguridad de la información o al punto de contacto seguridadinformacion@eppetroecuador.ec para su registro y correspondiente gestión.

7.19. Los funcionarios deben utilizar las cuentas de usuario y perfiles de acceso asignados únicamente para el cumplimiento de sus funciones y asignaciones de trabajo y serán responsables de su utilización y seguridad.

7.20. Al término de la relación laboral o movimiento de personal, la información institucional a cargo del servidor saliente deberá ser entregada al nivel de supervisión correspondiente quien la mantendrá bajo su custodia hasta que se entregue al nuevo servidor. La devolución de activos institucionales, servicios y recursos tecnológicos, deberá realizarse conforme lo establecido en el proceso "*GTH.05 Desvinculación del Personal*".

7.21. Los propietarios y custodios de información física y digital, deberán gestionar e implementar las medidas de protección específicas sobre la información confidencial y reservada conforme la competencia de las unidades orgánicas y de negocio respectivas.

7.22. Todo usuario de tipo Administrador creado por los fabricantes de software o hardware a utilizarse en la empresa deberá ser desactivado y en su defecto deberá generarse un usuario avanzado o de administración con los roles correspondientes.

7.23. Los permisos de usuario avanzado o de administración a las aplicaciones de los sistemas de control y adquisición de datos, base de datos, computadores de escritorio y portátiles, redes inalámbricas y demás componentes tecnológicos deben ser autorizados por el Jefe de la unidad orgánica y de negocio respectiva; y deberá contar con la motivación o justificación pertinente.

7.24. La adquisición, construcción, o adopción de todo software deberá contar con el aval previo y expreso de la Subgerencia de Tecnologías de la Información y Comunicación, y de la Unidad orgánica o de negocio solicitante; y, en casos que se requieran, con el aval del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), y este deberá ser probado funcional y técnicamente, en los ambientes correspondientes, previo a ser puesto en producción.

7.25. Los Usuarios funcionales responsables de los sistemas empresariales deben identificar las transacciones críticas a fin de que la Subgerencia de Tecnologías de la Información y Comunicación pueda incorporar los mecanismos de auditoría (logs) que permitan asegurar la trazabilidad de la información ante cualquier evento, cambio o modificación.
7.26. Todos los sistemas informáticos desarrollados, adquiridos o en suscripción deben poseer un módulo de auditoría de las actividades de todos los usuarios en el mismo, que permita conocer la trazabilidad, errores y advertencias ocurridos en el sistema.
7.27. Toda petición de acceso a sistemas empresariales deberá ser gestionado por el canal definido por la Subgerencia de Tecnologías de la Información y Comunicación.
7.28. Todo aplicativo desarrollado internamente o implementado por un tercero, deberá contar con la designación de un administrador funcional y un administrador técnico.
7.29. El Administrador funcional de aplicaciones empresariales será responsable de definir los roles y perfiles en los sistemas empresariales de acuerdo a las necesidades del negocio y analizar la pertinencia de asignarlos a un usuario en los aplicativos de la EP Petroecuador.
7.30. Con el objetivo de proteger la información sensible y garantizar un entorno de trabajo seguro, todo el personal debe mantener un escritorio limpio y ordenado, así como, la pantalla de los equipos libre de contenido y accesos innecesarios. Al finalizar la jornada laboral o en ausencia prolongada, los documentos físicos deben ser archivados de manera segura, y la información confidencial almacenada ya sea en dispositivos electrónicos protegida mediante contraseñas y bloqueos de pantalla o bajo llave. No se deben dejar credenciales de acceso, dispositivos extraíbles o material sensible expuesto sobre los escritorios.
7.31. En el caso de adquisición de bienes tecnológicos o prestación de servicios tecnológicos a terceros, dichos procesos y vínculos contractuales deberán observar que se lo realicen con proveedores que garanticen que los datos se encuentran en centros de cómputo que cumplan con estándares internacionales de seguridad y protección, especialmente para aquellos clasificados como confidenciales o reservados
7.32. Los responsables de los Macro procesos y Procesos deberán generar e implementar directrices específicas, procedimientos, formatos, guías o demás documentos normativos relacionados que sean de propósito específico y que le permitan la ejecución de acciones para salvaguardar la información digital o física que custodian y de los recursos tecnológicos institucionales que administra, gestiona o utiliza.
7.33. Todos los funcionarios de la empresa y usuarios externos deben dar especial atención en el tratamiento y protección interna de los datos personales en reposo, transferencia y uso, quienes, además de utilizar técnicas de protección deberán mantener la privacidad y trazabilidad de dichos datos.

8. Responsabilidades

Gerencia General

8.1. La Máxima Autoridad de la empresa se compromete a liderar el cumplimiento del Sistema de Gestión de Seguridad de la información de la organización.
8.2. La Gerencia General asignará los recursos necesarios, para el mantenimiento del Sistema de Gestión de Seguridad de la información (SGSI), previo al análisis realizado por el Comité de Seguridad de la Información.
8.3. La Gerencia General es responsable de aprobar la Política de Seguridad de la Información y cualquier cambio a la misma, así como las recomendaciones presentadas por el Comité de Seguridad de la Información, para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades de cada área

operativa o administrativa de la Empresa; y, promover la difusión, apoyo y cumplimiento de los establecido en la presente política.

8.4. La Gerencia General de la empresa designará un Oficial de Seguridad de la Información (OSI), quien coordinará con las unidades orgánicas y de negocio correspondientes, la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la EP PETROECUADOR, conforme las directrices de los entes de control.

Comité de Seguridad de la Información

8.5. El Comité de Seguridad de la Información será responsable de velar por la aplicación de la presente política.

8.6. Revisar la Política de Seguridad de la Información previo a la aprobación de la Máxima Autoridad.

8.7. Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad.

8.8. Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad de la información.

Procuraduría

8.9. La Procuraduría deberá brindar el apoyo y asesoramiento a los propietarios de información durante el proceso de clasificación de información de acuerdo a la legislación y normativa legal vigente.

Niveles de Supervisión, Dirección y Máximas Autoridades de Unidades Orgánicas y de Negocio.

8.10. Las Máximas Autoridades de las Unidades Orgánicas y de Negocio, deberán promover con su equipo de trabajo el cumplimiento de la presente política y demás normativa interna a fin de proteger la información empresarial que se encuentra bajo su custodia y evitar la ocurrencia de incidentes de seguridad de la información.

8.11. Los responsables de los macroprocesos, procesos y subprocesos de la empresa deberán identificar los riesgos de seguridad de la información y gestionar su tratamiento en los procesos incluyendo aquellos que tengan interacción con proveedores o terceros, así como los activos de información involucrados que son vulnerables y que causarán impacto a la empresa si se ven comprometidos.

8.12. Las jefaturas inmediatas, en ejercicio de sus roles de revisión y supervisión, aprobarán o negarán las peticiones de accesos lógicos para la ejecución de transacciones y operaciones en los sistemas de la empresa.

8.13. Todos los niveles de supervisión, en ejercicio de sus atribuciones, aplicarán los mecanismos definidos por la Subgerencia de Talento Humano, para emprender acciones contra servidores públicos que hayan cometido una violación a la seguridad de la información de forma tal que se garantice la continua y permanente seguridad de la información.

8.14. Los responsables de los procesos deberán determinar los procesos críticos de la empresa, elaborando el Análisis de Impacto del Negocio, a fin de determinar los requisitos para la continuidad de las operaciones y la disponibilidad de la información en situaciones adversas, por ejemplo, durante una interrupción de crisis o desastre.

8.15. Las jefaturas inmediatas son responsables de verificar el buen uso de la información, asociada a los procesos y servicios bajo su responsabilidad, por parte del personal de la institución y personal externo autorizado a su cargo (proveedores nacionales o internacionales, pasantes o consultores).

8.16. Los propietarios de la información empresarial, serán los encargados de levantar y actualizar el inventario de los activos de información a su cargo, así como su clasificación, con el apoyo metodológico de Seguridad de la Información, Gestión Documental y Procuraduría.

Subgerencia de Tecnologías de la Información y Comunicaciones

8.17. Es responsable de implementar y determinar las medidas de seguridad tecnológica producto del análisis de riesgos de seguridad de la información, con la finalidad de proteger la integridad, disponibilidad y confidencialidad de la información digital almacenada en la infraestructura tecnológica.
8.18. Gestionar los niveles de acceso e identidad lógica de acuerdo a las necesidades de los propietarios de la información o procesos para lo cual definirá la correspondiente normativa específica.
8.19. Identificar, evaluar y dar tratamiento a los riesgos de ciberseguridad a la que se encuentre expuesta la infraestructura tecnológica a fin de minimizar la ocurrencia de un ataque digital a la infraestructura y servicios tecnológicos de la empresa.
8.20. Implementar las medidas técnicas preventivas ante amenazas cibernéticas que permitan detectar, proteger, responder y recuperar los sistemas de información e información digital frente a incidentes de ciberseguridad.
8.21. Debe asegurar mediante los mecanismos apropiados, que todo medio de almacenamiento que deba salir de la empresa, incluyendo garantía técnica o cumplimiento de vida útil, mantenga una adecuada cadena de custodia y de ser necesario, sea sometido a un procedimiento de destrucción lógica, para evitar fuga de información.
8.22. Debe establecer y documentar los procedimientos de control de accesos lógicos con base en los requisitos del negocio y de seguridad de la información; incluidos los controles para accesos privilegiados, considerando la estrategia de seguridad del menor privilegio, la cual se centra en garantizar que las identidades, las personas y los procesos reciban el nivel mínimo de permisos necesarios para ser productivos.
8.23. La Subgerencia de Tecnologías de la Información y Comunicación, y la Jefatura de Gestión Documental establecerán controles técnicos o documentos de normativa interna para la transferencia de información digital y física a todas las partes interesadas internas y externas que se encuentren al amparo de contratos, convenios o acuerdos de intercambio de información.
8.24. La Subgerencia de Tecnologías de la Información y Comunicación, conjuntamente con Procuraduría documentarán e implementarán los procedimientos apropiados para proteger los derechos de propiedad intelectual de los sistemas o aplicaciones desarrolladas en la empresa.
8.25. Debe establecer las metodologías para el desarrollo seguro de aplicativos informáticos, así como los estándares y medidas de seguridad para dicha ejecución.
8.26. Debe aplicar los mecanismos correspondientes para eliminar o enmascarar datos considerados como sensibles previo al uso de la información en ambientes no productivos, estos datos deben ser identificados por el propietario de la información

Subgerencia de Logística y Abastecimiento

8.27. Es la encargada de administrar los aplicativos informáticos de la empresa que soportan el proceso de Gestión Documental y generar la normativa correspondiente que deberá estar alineado al SGSI empresarial, así como de custodiar los diferentes catastros documentales y su respectiva seguridad. PCA.04.DR.02

8.28. Es responsable de establecer los lineamientos para la custodia y protección del inventario de documentos físicos y digitales que forman parte del archivo central y de gestión, incluyendo su etiquetado.
8.29. Deberá establecer mecanismos que garanticen la inclusión en la gestión de incidentes a los contratistas relacionados, a fin de que notifiquen incidentes relacionados a la alteración o mal uso de información, incluyendo la fuga, cuando éstos fueran testigos; dicha notificación se efectuará al administrador del contrato.

Subgerencia de Talento Humano

8.30. Es responsable de custodiar los diferentes tipos de expedientes personales de los servidores públicos y obreros activos y ex trabajadores a nivel nacional conforme la clasificación y normativa legal pertinente.
8.31. Debe verificar los antecedentes y asegurar la idoneidad de todos los candidatos a funcionarios de la empresa teniendo en cuenta la norma legal vigente y ética aplicable a fin de minimizar riesgos de seguridad de la información.
8.32. Debe establecer los mecanismos para concientizar, formar y educar al personal sobre las responsabilidades, reglas y obligaciones de seguridad de la información aplicables.
8.33. Debe establecer las reglas que permitan establecer las condiciones de acceso y no divulgación a la información en custodia del personal, así como formalizar, comunicar y socializar los procesos disciplinarios para tomar acciones contra el personal e involucrados que hayan cometido una violación de la política de seguridad de la información, de acuerdo a la norma legal vigente.
8.34. Debe coordinar con la Subgerencia de Tecnologías de la Información y Comunicación y Jefatura de Seguridad Física los mecanismos oportunos para controlar de manera automatizada la aplicación de los procesos de vinculación, movimientos y desvinculación de personal a fin de que se minimicen los riesgos asociados al mal uso de permisos de acceso lógico y físico, roles asignados y mal uso de la información.
8.35. Debe definir, comunicar y socializar al personal de la empresa las responsabilidades y deberes en relación a la seguridad de la información, incluso aquellas que siguen siendo válidas aún después de la terminación de la relación laboral.
8.36. Debe definir las condiciones y restricciones para las actividades de trabajo a distancia, considerando los requisitos de seguridad física del entorno, seguridad de las comunicaciones, y la sensibilidad de la información física o digital.

Jefatura de Seguridad y Transparencia de la Información

8.37. Es responsable de la gestión del Sistema de Seguridad de la Información (SGSI), de la gobernanza y de definir normativa y lineamientos generales para la gestión de la seguridad de la información empresarial, y de realizar controles y evaluaciones internas que permitan verificar el correcto funcionamiento del SGSI empresarial y de sus procedimientos relacionados.
8.38. Evaluar el cumplimiento y eficacia de los controles de seguridad de la información, así como coordinar la evaluación interna del Sistema de Gestión de Seguridad de la información (SGSI) de forma periódica.
8.39. Notificar a los funcionarios de la empresa mediante correo electrónico, respecto de las infracciones de confidencialidad, incumplimiento a normativa interna relacionada a seguridad de la información o uso indebido de la información institucional que se identifiquen en las evaluaciones de controles de seguridad, con la finalidad de establecer un antecedente y prevenir futuras conductas inadecuadas y vulneración de la confidencialidad de la información.

8.40. Asesorar y coordinar la identificación y gestión de riesgos de seguridad de la información de la EP Petroecuador, para lo cual, mantendrá actualizada la metodología de gestión de riesgos.
8.41. Gestionar la preparación, detección, evaluación y respuesta ante la ocurrencia de incidentes de Seguridad de la Información empresarial en coordinación y apoyo de las unidades orgánicas y de negocio de la EP Petroecuador.
8.42. En virtud de sus atribuciones, ante un evento o incidente de seguridad de la información detectado, podrá acceder a los registros de auditoría de los sistemas informáticos, información custodiada por el personal de la empresa en dispositivos de almacenamiento, computadores u otros medios, o podrá solicitar información a las unidades orgánicas y de negocio, misma que deberá ser entregada oportunamente y sin restricción alguna.
8.43. Coordinar la revisión y actualización de la Política de Seguridad de la Información, con la finalidad de realizar ajustes necesarios de mejora al menos una vez al año y cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico en el entorno de la EP PETROECUADOR.

Jefatura de Imagen y Comunicación

8.44. De acuerdo a sus atribuciones, debe establecer y mantener los canales de comunicación empresarial, incluyendo el envío masivo de mensajes por correo institucional. A través del análisis de riesgos de imagen deberá autorizar o denegar las peticiones de buzones de correo para envío masivo de información.
8.45. Mantener preparado un plan de comunicación ante incidentes de seguridad de la información, dependiendo de su naturaleza e impacto.

Jefatura de Seguridad Física

8.46. Determinar y mantener las medidas de seguridad físicas perimetrales y del entorno a la empresa, incluidos los diferentes sitios donde se encuentra el personal para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la empresa.
8.47. Identificar las instalaciones críticas y monitorearlas de acuerdo a los riesgos identificados en el ámbito de competencia de seguridad física.

Jefatura de PMO Empresarial

8.48. Determinar y socializar los lineamientos para que en la empresa se identifiquen y traten oportunamente los riesgos de seguridad de la información en todas las etapas que correspondan de un proyecto.
8.49. El gerente de proyecto gestionará los riesgos de Seguridad de la Información en calidad de propietario del riesgo hasta el cierre del proyecto, en caso de existir riesgo residual no aceptable este deberá transferirse al proceso dueño del proyecto y notificarse a la Jefatura de Seguridad de la Información para el respectivo seguimiento.

Oficial de Seguridad de la Información

8.50. Asesorar y coordinar con el equipo técnico designado por el Comité de Seguridad de la Información, la ejecución periódica de la metodología de Gestión de Riesgos de Seguridad de la Información.
8.51. Coordinar acciones e informar al Comité de Seguridad de la Información de las acciones de recuperación de los servicios tecnológicos cuando se presenten incidentes de seguridad de la información de prioridad crítica que afecten la continuidad de las operaciones de la empresa o una vez que haya sido declarado un evento de crisis.

8.52. Las establecidas en la Sección II Capítulo I del Reglamento del Comité de Seguridad de la Información (GOB.DR.02).

Personal de EP PETROECUADOR

8.53. Todo el personal de la EP PETROECUADOR debe conocer y cumplir las disposiciones descritas en la presente política, así como las leyes y normativa conexa, consecuentemente, asumirán la responsabilidad de evitar que se produzcan violaciones de la normativa que rige en la empresa. Dicho incumplimiento dará lugar a la aplicación del régimen disciplinario y Reglamento Interno de Trabajo de la EP PETROECUADOR, previa aplicación del debido proceso.

8.54. Todo el personal es responsable de tomar conocimiento de las comunicaciones emitidas en materia de seguridad de la información y de asistir o realizar los cursos de capacitación que se pongan a disposición.

8.55. Todo el personal de la EP PETROECUADOR, debe aplicar las reglas, procesos y procedimientos relacionados a esta política con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información empresarial.

8.56. Tanto el personal de la EP PETROECUADOR como sus contratistas, proveedores, y/o cualquier tercero que, en razón de la aplicación de diferentes instrumentos jurídicos tengan autorización para ingresar o permanecer en las instalaciones de la EP PETROECUADOR, son responsables de dar cumplimiento a las normas, procesos y procedimientos establecidos en la empresa referentes al adecuado uso y manejo de la información, a fin de mantener las salvaguardas necesarias para proteger la información tanto física como digital que soporta sus operaciones.

8.57. Todo el personal tendrá bloqueado el uso de medios de almacenamiento extraíbles como: USB, discos externos, CD/DVD/SD u otros medios; cuando sea autorizado de forma excepcional y temporal por necesidad institucional el uso de los medios de almacenamiento extraíbles, la autorización deberá estar debidamente justificada y aprobada por los Gerentes de las Unidades Orgánicas y de Negocio. La Subgerencia de Tecnologías de la Información y Comunicación, implementará los medios que permitan mantener los registros de auditoria de la transferencia de información a dichos medios de almacenamiento.

8.58. La Gerencia General y Gerencias de las Unidades Orgánicas y de Negocio, mantendrán pre-aprobación de uso de medios de almacenamiento extraíbles, la Subgerencia de Tecnologías de la Información y Comunicación, mantendrá los registros de auditoria de la transferencia de información a dichos medios de almacenamiento.

9. CUMPLIMIENTO DE NORMATIVA

9.1. EP PETROECUADOR se compromete a cumplir con todas las normativas legales y regulaciones aplicables en materia de seguridad de la información, incluidas, pero no limitadas a:

- Código Orgánico Integral Penal
- Ley Orgánica de Protección de Datos Personales
- La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)
- Esquema Gubernamental de Seguridad de la Información (Acuerdo Ministerial 2024 - 0003)
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley de Seguridad Pública y del Estado.
- Normas de Control Interno - CGE

- Reglamento General de la Ley Orgánica de Telecomunicaciones
- Estándares nacionales o internacionales, como la NTE INEN ISO/IEC 27000, y cualquier otra normativa o ley relacionada que regule la seguridad y protección de los datos personales y sistemas en el sector público.

10. RESTRICCIONES Y PROHIBICIONES

10.1. Con el fin de garantizar la seguridad de la información empresarial, se encuentra prohibido usar los recursos físicos o tecnológicos de la empresa para las siguientes actividades:

- Promover de cualquier forma, la explotación sexual, racismo o violencia.
- Promover el uso ilegal de sustancias estupefacientes y psicotrópicas, drogas o armas de fuego.
- Enviar mensajes discriminatorios con relación a ideología, afiliación política o sindical, orientación sexual, etnia, estado de salud, religión, nacionalidad, condición migratoria.
- Promover o posibilitar juegos o apuestas en línea.
- Hacer uso de software que contenga cualquier tipo de código malicioso (virus, programas que se auto replican, programas espías, programa de captura de credenciales, etcétera).
- Intentar vulnerar la seguridad de las aplicaciones, servicios o equipos de propiedad de la empresa.
- Envió de texto difamatorio, ofensivo, intimidatorio o injurioso contra la honra de las personas.
- Envío de email masivo, cadenas de correos, spam, relacionado a propaganda comercial, gremial, partidista o política.
- Retiro o salida de documentos físicos o digitales de las instalaciones, sin la debida autorización y aplicación del proceso correspondiente.
- Acceder a una cuenta de correo electrónico institucional que pertenezca a otro servidor o personal externo autorizado.
- Registrar la cuenta de correo electrónico institucional en sitios de Internet de acceso público o privado que no se relacionen con la actividad laboral, ya que representa un riesgo de seguridad y ser objeto de robo o venta de información.
- Los usuarios se abstendrán de abrir mensajes de correo o documentos adjuntos en los que el remitente sea desconocido o sospechoso, para evitar infecciones de virus o malware que pueda comprometer la información del usuario y de la empresa, caso contrario asume la responsabilidad por las consecuencias que puedan ocasionar la ejecución de los archivos adjuntos.

ACTA DE APROBACIÓN

RESPONSABLE(S)	FIRMA(S)
APROBADOR(ES) *Responsable del Macroproceso o su delegado, conforme resolución vigente y/o acta de designación de responsables de procesos.* El(Los) suscrito(s) aprueba(n) este documento para su formalización y publicación en la Normativa Interna de Gestión.	Firmado electrónicamente por: LEONARD BRUNS Validar únicamente con FirmaEC **Cargo:** Gerente General Firmado electrónicamente por: ALBA NATHALI BALSECA LOZADA Validar únicamente con FirmaEC **Cargo:** Subgerente de Planificación y Control de Gestión
ELABORADOR(ES) Y REVISOR(ES) DEL ÁREA(S) USUARIA(S) *Delegado(s) del Responsable del Proceso o su delegado* El(Los) suscrito(s) dejan constancia de la elaboración y/o revisión de este documento para su formalización y publicación en la Normativa Interna de Gestión.	Firmado electrónicamente por: MARIA BELEN LLERENA VELASCO Validar únicamente con FirmaEC **Cargo:** Jefe de Seguridad y Transparencia de la Información (Oficial de Seguridad de la Información) Firmado electrónicamente por: SANTIAGO ALEJANDRO PINTO USUAY Validar únicamente con FirmaEC **Cargo:** Analista de Seguridad de la Información
REVISIÓN LEGAL *Área Legal* El(Los) suscrito(s) deja(n) constancia del asesoramiento a los responsables de los macro procesos y procesos en la legislación aplicable vigente. De acuerdo con la Norma de Control Interno número 200-06: "*Competencia profesional*", emitida por la Contraloría General del Estado, sin que se pueda extender su participación sobre el análisis o validación de aspectos técnicos o económicos. La revisión efectuada se limita a las modificaciones solicitadas por el área requirente, conforme consta en la hoja de control de cambios; y, a las responsabilidades señaladas en el Proceso ASE.01 Gestión de Asuntos Jurídicos; y, ASE.PR.01 Requerir y Actualizar Procesos, Procedimientos y/o Documentos Relacionados.	Firmado electrónicamente por: CAROLINA MERCEDES ESTRELLA BUSTAMANTE Validar únicamente con FirmaEC **Cargo:** Jefe de Asesoría y Normas Laborales Firmado electrónicamente por: MARIA JOSE TRUJILLO JARAMILLO Validar únicamente con FirmaEC **Cargo:** Abogado de Relaciones Laborales
REVISIÓN METODOLÓGICA *Área de Gestión por Procesos* El(Los) suscrito(s) deja(n) constancia de la revisión de los aspectos metodológicos de la Gestión por Procesos. De acuerdo con la Norma de Control Interno número 200-06: "*Competencia profesional*", emitida por la Contraloría General del Estado, sin que se pueda extender su participación sobre el análisis o validación de aspectos técnicos o económicos.	Firmado electrónicamente por: CHRISTIAN HERNAN AMADOR CHAMORRO Validar únicamente con FirmaEC **Cargo:** Jefe de Gestión por Procesos Firmado electrónicamente por: ADRIANA GRACIELA MELENA HEREDIA Validar únicamente con FirmaEC **Cargo:** Analista de Gestión por Procesos