1. INTRODUCCIÓN

Las políticas de seguridad de la información consisten en medidas de prevención que se toman con el fin de mantener la seguridad y la privacidad en la información de los procesos que se manejan. Sirve para mantener el buen funcionamiento y uso de la tecnología en la compañía, así como la buena ética del manejo de esta, teniendo en cuenta las prevenciones en los procedimientos que se realizan. Es así, que para la CORPORACIÓN CLUB SOCIAL Y DEPORTIVO ECOPETROL BOGOTÁ, la política de seguridad de la información surge como un lineamiento estratégico dada su relevancia.

2. OBJETIVO

Establecer, implementar, mantener, mejorar y socializar los lineamientos para la seguridad de la información por medio de una lectura fácil de comprender que evite riesgos y garantizar la seguridad de la misma; Esto con la finalidad de tener un adecuado manejo de los colaboradores de la organización.

3. ALCANCE

Aplica a todos los equipos o redes de la compañía a las que se tengan acceso, así como a todos los procesos, actividades de negocio y a todas las personas que directa o indirectamente prestan algún servicio para el Club Ecopetrol Bogotá.

El incumplimiento de lo estipulado en el presente manual acarrea sanciones disciplinarias de acuerdo con las obligaciones, deberes y responsabilidades definidas.

4. LINEAMIENTO GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Club Ecopetrol Bogotá, consiente del valor de la información, como activo vital, siendo una herramienta de gran importancia para la toma de decisiones y en cumplimiento de su

misión, visión y valores corporativos, protege la información propia y en custodia, garantizando adecuados niveles de:

- **Confidencialidad**, garantizando el acceso sólo para los usuarios autorizados.
- **Integridad**, evitando modificaciones no autorizadas.
- **Disponibilidad**, garantizando que la información esté disponible cuando se necesite.

Tomando como base que la efectividad de la política depende del comportamiento de las personas, (por lo que saben, lo que sienten y de que estén dispuestos a realizar) y los controles establecidos en las políticas de seguridad descritas en el presente documento.

5. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se relacionan algunas acciones identificadas que afectan la disponibilidad, confidencialidad e integridad y que ponen en riesgo la Seguridad de la Información:

a. Permitir que personas ajenas al Club Ecopetrol Bogotá ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.

b. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
c. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
d. Reutilizar papel que contenga información sensible.
e. Dejar documentos o notas escritas con información sensible sobre las mesas.
f. Dejar en los equipos destinados a capacitación información sensible o confidencial.
g. Hacer uso de la red de datos del Club Ecopetrol Bogotá, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
h. Instalar software en la plataforma tecnológica del Club Ecopetrol Bogotá, cuyo uso no esté autorizado por la Oficina de Informática y Sistemas, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
i. Enviar información clasificada del Club Ecopetrol Bogotá por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
j. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos del Club Ecopetrol Bogotá, para beneficio personal.
k. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.
l. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
m. Retirar de las instalaciones del Club Ecopetrol Bogotá computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.
n. Ejecutar acciones para eludir y/o modificar los controles establecidos en el presente manual de Seguridad de la Información.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

6. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de la información está compuesta por:

a. El COE (Comité Operativo de Emergencias)
b. El Oficial de Seguridad de la Información.
c. El líder o propietario de cada proceso
d. Los propietarios de los activos de Información

El oficial de seguridad de la información o quien haga sus veces, podrá asistir cuando el COE se reúna con el propósito de tratar temas de seguridad digital y de la información o relacionadas con estas.

El Comité Operativo de Emergencias se reunirá ordinariamente por lo menos una vez (1) cada tres meses, con la mitad más uno de sus miembros, y sus decisiones serán tomadas por la mayoría simple, pero podrá reunirse extraordinariamente cada vez que sea necesario. A dichas reuniones podrán asistir como invitadas las personas que se consideren necesarias de acuerdo con los asuntos a debatir.

7. LINEAMIENTOS GENERALES

7.1 LINEAMIENTO CONTROL DE ACCESO A LOS SISTEMAS

Los coordinadores o líderes de procesos junto con el área de Sistemas deben determinar las reglas de control de acceso apropiadas de acuerdo con las actividades que desarrolla cada uno de los funcionarios, según su rol dentro de la compañía y evaluando los riesgos asociados al uso de esta. Por lo tanto, son ellos quienes autorizan o retiran los permisos para el uso de un activo de información teniendo en cuenta lo establecido en:

a. Los procedimientos de control de acceso físico definidos.
b. El acceso a servidores, bases de datos, Internet, correo electrónico y aplicaciones deben realizarse bajo los lineamientos definidos y establecidos por el proceso de Sistemas.
c. La administración de usuarios debe realizarse bajo los lineamientos definidos por el proceso de Sistemas
d. Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
e. Todas las contraseñas utilizadas por usuarios y administradores de sistemas deben cumplir con los lineamientos definidos por el área de Sistemas descritos en el presente documento.

7.2 LINEAMIENTO USO ADECUADO DE LOS RECURSOS

Los funcionarios, contratistas y/o terceros tendrán a su disposición el uso de recursos tecnológicos y/o de infraestructura, de acuerdo con las funciones laborales que así lo requieran, para el uso de estos recursos, los funcionarios, contratistas y/o terceros aceptan y se acogen a las Políticas de Seguridad de la Información incluyendo el cumplimiento de las siguientes responsabilidades o deberes:

a. Los recursos deben usarse estrictamente para fines laborales y nunca deben transmitir, procesar y/o almacenar información personal.
b. No se permite transmitir, almacenar y/o procesar información que atente contra la propiedad intelectual o derechos de autor.
c. Se prohíbe la transmisión, almacenamiento y/o procesamiento de SPAM (Correo no deseado o no solicitado) y/o cualquier tipo de archivo de procedencia desconocida o infectado con algún tipo de software malicioso.
d. Se prohíbe la transmisión, almacenamiento y/o procesamiento de material relacionado con pornografía, armas, alcohol o actividades ilícitas.
e. Se prohíbe el uso e instalación de software ilegal o sin licenciar, al igual que todo tipo de programas (Keyloggers, Crackers, entre otros.) que atenten o faciliten la perdida de la integridad, disponibilidad o confidencialidad de la información.
f. Los recursos tecnológicos pueden ser accedidos y monitoreados por un ente de control del Club Ecopetrol Bogotá, sin incurrir en violación de la privacidad, puesto que dichos recursos son asignados para la labor contratada.
g. La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad exclusiva del área de Sistemas, por tanto, son los únicos autorizados para realizar esta labor.
h. Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.
i. Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren

del puesto de trabajo.

j. Los requerimientos de recursos tecnológicos de las diferentes áreas deben ser avalados por el área de Sistemas.
k. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por el área de Sistemas y mantenimiento.
l. Los equipos de cómputo asignados deben ser devueltos al área de Sistemas una vez sean reemplazados o cuando el funcionario o contratista responsable de dicho equipo finalice su vinculación con el Club Ecopetrol Bogotá.
m. De acuerdo con el literal anterior, el Club Ecopetrol Bogotá no debe almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de estos.

7.3 LINEAMIENTO USO CORREO ELECTRÓNICO

La asignación de una cuenta de correo electrónico del Club Ecopetrol Bogotá se da como herramienta de trabajo para cada uno de los funcionarios qude la requieran dentro del desempeño de sus funciones, así como a contratistas que lo requieran para el desempeño de su labor; su uso se encuentra sujeto a las siguientes reglas:

a. El correo electrónico debe utilizarse únicamente para labores propias de la Corporación.
b. No se debe enviar información de la entidad a cuentas de correo personales o divulgar información de esta en las redes sociales, excepto aquellas que, por motivo de la operación del Club Ecopetrol Bogotá, se han establecido con los clientes o terceros y autorizados por el área de comunicaciones y/o gerencia.
c. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Corporación y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

7.3.1. No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:

a. Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
b. Enviar mensajes no autorizados con contenido religioso o político.
c. El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por el área de Sistemas.
d. Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos: El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
e. El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
f. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
g. Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

7.4 LINEAMIENTO USO DE RED E INTERNET

El uso de la red e Internet como herramienta de trabajo permite a los funcionarios y contratistas acceder a sitios relacionados con el desarrollo las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica

y monitorea, considerando para todos los casos, las siguientes normas:

a. Todos los accesos a internet de los equipos institucionales deben ser realizados a través de los canales provistos por la Corporación.
b. La navegación en Internet es controlada de acuerdo con las restricciones definidas para los usuarios y está destinada únicamente a las actividades laborales de la Corporación.
c. No se permite la navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
d. No se permite la publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
e. No se permite la descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
f. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

7.5 LINEAMIENTO USO COMPUTADORES PORTÁTILES Y DE ESCRITORIO

a. Cada usuario es responsable de velar por el respaldo de la información de sus equipos de trabajo.
b. Los usuarios deben bloquear la sesión de sus equipos de trabajo, cuando se ausenten de su puesto.
c. Los equipos que hacen parte de la infraestructura tecnológica del Club Ecopetrol Bogotá, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado a los mismos.
d. El Club Ecopetrol Bogotá, adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.
e. Los funcionarios y contratistas velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
f. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática y Sistemas, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

7.6 LINEAMIENTO USO DISPOSITIVOS MÓVILES

a. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.
b. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por el área de Sistemas, previa autorización del jefe inmediato y la verificación de contar con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la información y la infraestructura que la contiene.

7.7 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

a. Los usuarios que requieran usar los equipos fuera de las instalaciones del Club Ecopetrol deben velar por la protección de estos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información sensible.
b. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento
c. Gestión de Incidentes de Seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.
d. Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del Club Ecopetrol Bogotá deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

7.8 LINEAMIENTO USO DE COMPUTACIÓN EN LA NUBE

a. El Club Ecopetrol Bogotá, podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.
b. Los servidores públicos y contratistas no tienen permitido almacenar información en la nube (Dropbox, Onedrive y similares) que no hayan sido autorizados por la Gerencia.

7.9 LINEAMIENTO DEE CONTROL DE ACCESO

a. Para el ingreso al Datacenter se deberá contar con autorización del área de Sistemas y/o gerencia, reportando el ingreso en el formato para dicho fin.
b. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática y Sistemas de la Corporación deberá estar creado previa autorización coordinación de talento humano.
c. Los equipos de contratistas y demás terceros que requieran acceder a las redes de datos de la Corporación deben cumplir una de verificación de cumplimiento de informática antes de concedérseles dicho acceso, realizada por el área de sistemas.

7.10 LINEAMIENTO DE ESCRITORIO LIMPIO Y PANTALLA DESPEJADA

Todos los funcionarios, Contratistas o terceros que hagan uso de la infraestructura de la Corporación, para el desarrollo de sus labores deben:

a. Mantener la información objeto de su labor debidamente custodiada y salvaguardada del acceso de personas no autorizadas, de acuerdo con la clasificación de los activos de información.
b. Conservar la pantalla libre de accesos directos a información clasificada como Confidencial.
c. Verificar que en los equipos asignados o bajo su responsabilidad se bloquee la sesión de trabajo, cuando se ausenten.

d. Evitar que los documentos que contengan información clasificada como Confidencial, se expongan en las impresoras, fax, fotocopiadoras y escáneres.
e. En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
f. Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.
g. Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
h. No se deberá reutilizar papel que contenga información sensible.
i. Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.
j. Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

8. RESPALDO DE INFORMACIÓN

El Club Ecopetrol Bogotá velara por la conservación de la información, realizando copias de respaldo de esta, para tal fin, el área de Sistemas es responsable de aplicar el proceso definido para ello, teniendo en cuenta:

a. El área de Sistemas garantizara las copias de seguridad custodiadas en one drive, carpetas compartidas, servidores; es así, que toda información que sea guardada localmente no cuenta con copia de seguridad por lo cual, el usuario deberá garantizar que la información requerida para la labor se encuentre archivada en one drive o carpetas compartidas.
b. Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
c. Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia.
d. El área de Sistemas del Club Ecopetrol Bogotá, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación, y definirá conjuntamente con las dependencias los períodos de retención de esta.

9. USO DE CONTRASEÑAS

Toda cuenta de usuario es de uso personal e intransferible, su utilización debe ser exclusiva para fines laborales objeto de la labor contratada. Como una de las buenas prácticas para el aseguramiento de la información propia, los funcionarios, contratistas o terceros que hacen uso de la infraestructura tecnológica del Club Ecopetrol Bogotá son responsables de:

a. Mantener la confidencialidad de las contraseñas.
b. Evitar conservar registros físicos de las contraseñas.
c. No compartir la contraseña de sus cuentas de usuario asignadas.

9.1 SELECCIÓN DE CONTRASEÑAS

Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

a. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
b. Las contraseñas no deberán ser reveladas.
c. Las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones (Correo Electrónico, Orfeo, etc); igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
d. Cualquier incidente de seguridad de información que se presente por el mal uso de una contraseña, será responsabilidad del propietario de la cuenta y deberá ser informado a Seguridad de la información.

Las contraseñas se deberán cambiar con una periodicidad semestral, y deberán cumplir:

- Mínimo 8 caracteres.
- Letras mayúsculas.
- Letras minúsculas.
- Números.
- Caracteres especiales.

10. GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

La gestión de riesgos de seguridad de la información forma parte de la cultura organizacional y se promueve a todos los niveles del Club Ecopetrol Bogotá, cuyo fin es garantizar el cumplimiento de los objetivos dentro de un ámbito de seguridad que permita la menor exposición al riesgo dentro de los criterios establecidos.

Para su cumplimiento la Alta Dirección, es la responsable de proveer y garantizar los recursos necesarios para la adecuada Gestión de Riesgos de Seguridad de la Información, así como de velar por el cumplimiento de todas las actividades concernientes a la identificación, planeación, administración, seguimiento y control de los riesgos de seguridad de la información.

La gestión de riesgos de seguridad de la información se realizará conforme a los lineamientos descritos en el Procedimiento de Gestión de Riesgos de Seguridad de la Información.

11. LINEAMIENTO DE TRABAJO REMOTO O TELETRABAJO

Considerando la necesidad de brindar agilidad en el desarrollo de las labores diarias del Club Ecopetrol Bogotá se permite el acceso desde redes externas solo en los siguientes casos:

Soporte técnico: Por parte del personal de tecnología para labores de soporte a la plataforma tecnológica, que estén justificadas con base en la criticidad de la operación o actividad a realizar.

Quienes deban realizar un tipo de conexión como los mencionados anteriormente deben estar autorizados por los líderes de los procesos correspondientes previo cumplimiento de las normas y lineamientos emanados por el área de Sistemas y solicitados formalmente mediante la herramienta que disponga el Club Ecopetrol Bogotá.

Cuando se establezcan contratos con terceros de monitoreo, soporte u operación de la plataforma tecnológica se deberán:

a. Establecer acuerdos de confidencialidad y manejo seguro de la información.
b. Limitar dentro del contrato los tipos de acceso que se tendrán y la responsabilidad del tercero con respecto a la información a monitorear o que reside en los equipos objeto de soporte u operación.

11.1 NORMAS BÁSICAS DE CONEXIÓN

Para los casos en los que se autorice el trabajo remoto o teletrabajo se tiene que cumplir con:

a. El teletrabajador debe resguardar la información institucional, impidiendo el acceso a terceras personas, en consecuencia, el acceso a la información de la Corporación será ejecutado bajo la responsabilidad del teletrabajador dando cumplimiento a las normas establecidas en la entidad.
b. El teletrabajador debe utilizar la información, incluyendo los datos personales, únicamente para las labores propias de su cargo.
c. El acceso de los teletrabajadores a los sistemas de información de la entidad se realizará a través de una VPN o mecanismo seguro aprobado por el área de Sistemas.
d. El teletrabajador debe cumplir las mismas medidas de seguridad definidas como si estuviera laborando en las instalaciones de la entidad.
e. Queda prohibido la cesión de cualquier tipo de datos a terceros, ni siquiera a efectos de conservación.
f. El teletrabajador debe evita compartir información de la entidad con familiares, amigos o terceros.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Todos los funcionarios y contratistas del Club Ecopetrol Bogotá, son responsables de reportar los eventos e incidentes de Seguridad.
d de Información de los cuales tengan conocimiento, es responsabilidad del grupo de Seguridad de Información gestionar el reporte e investigación de estos, de acuerdo con las siguientes definiciones:

a. **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio, red o del entorno que indica una posible violación de las políticas de seguridad de la información de la Corporación, falla en los controles o situación previamente desconocida que puede ser relevante para la seguridad de la información.
b. **Incidente de Seguridad de la Información:** Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones del Club Ecopetrol Bogotá y amenazan la confidencialidad, integridad y/o disponibilidad de la información.

Para dar cumplimiento a lo mencionado anteriormente se debe:

a. En todos los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática se deberán generar registros de eventos (logs) que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.
b. Todo evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado al Oficial de Seguridad de la información.

12.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a. Los funcionarios y contratistas del Club Ecopetrol Bogotá, deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
b. Para gestionar los incidentes de Seguridad de la Información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.
c. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
d. Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad de la Información para la Entidad.
e. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

13. LINEAMIENTO SEGURIDAD INFORMÁTICA

Para velar por la seguridad de la información se debe cumplir con las siguientes directrices las cuales buscan generar conciencia a los funcionarios y contratistas sobre la importancia y sensibilidad de los procesos y recursos críticos que permiten al Club Ecopetrol Bogotá, crecer y mantener su competitividad, para ello se debe garantizar la Seguridad Informática teniendo en cuenta lo siguiente:

13.1 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

a. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar ante posibles fallos ocasionados por código malicioso.
b. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización del área de Sistemas, y deberán ser actualizados permanentemente.
c. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.
d. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura la Corporación deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la

Información.

e. El Club Ecopetrol Bogotá será responsable de velar que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.
f. Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.
g. Los programas deberán ser ejecutados solamente por el área de Sistemas.

13.2 SEGURIDAD DE EQUIPOS DE CÓMPUTO

a. Habilitar y tener configurado en todos los equipos de escritorio y portátiles un software de firewall personal, cuyas reglas no puedan ser modificadas por los usuarios, ni detener el servicio.
b. Habilitar y tener configurado en todos los equipos de cómputo de la corporación, software de protección contra software malicioso, ajustado para actualizarse de forma automática y realizar evaluaciones periódicas de los sistemas, cuyas reglas no puedan ser modificadas por los usuarios, ni detener el servicio.
c. Deben estar activos los registros de auditoria localmente, se deben registrar los eventos de seguridad y aquellos que sean definidos en las guías de Hardening.
d. Realizar un borrado seguro para todo equipo (PC, Servidor, otros equipos asignados para el desarrollo de las labores diarias) que deba ser reasignado, trasladado o dado de baja.
e. Devolver el equipo al finalizar su relación contractual con el Club Ecopetrol

13.3 SEGURIDAD DE LA RED

a. Realizar la configuración de la seguridad en firewalls según Estándar de Seguridad de Firewalls, adicionalmente se debe validar que toda regla está documentada en el Firewall y que el uso de todos los protocolos se encuentre justificado.
b. Realizar una inspección semestral de la configuración de firewall y routers por parte del área de Sistemas.
c. Deshabilitar las cuentas de usuario innecesarias que los dispositivos de red traen incorporados de fábrica, deben ser modificados antes de su salida al ambiente de producción.
d. Asegurar que los servicios o aplicaciones que sean publicados para su acceso a través de la red cuenten con un nombre descriptivo a través del cual puedan ser identificados por medio de los servidores DNS locales, en lugar de utilizar la dirección IP donde se encuentre dicho servicio o aplicación.
e. Realizar pruebas de vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios por lo menos semestralmente.
f. Realizar una prueba de penetración anualmente o en caso de realizar cambios críticos en la infraestructura.
g. El área de control interno realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

13.4 DOCUMENTACIÓN DE PROCEDIMIENTOS OPERATIVOS

a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.
b. Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta

el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

c. Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

13.5 CONTROL DE CAMBIOS OPERATIVOS

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte del área de Sistemas, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.
b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de Control de Cambios. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

Para atender las solicitudes de soporte de los usuarios cuenta con varios niveles de Soporte Técnico que le ayudarán a resolver los problemas o tomar decisiones certeras de uso relacionadas con los equipos e infraestructura de cómputo, los niveles establecidos son:

c. Soporte Técnico Nivel 1: (*El soporte de primer nivel podrá ser desempeñado por un funcionario de planta o quien la entidad designe para el desarrollo de estas actividades*) Es el primer punto de contacto con el usuario, levantamiento del requerimiento o incidencia y determinación del problema. Consiste en atención en primera instancia siendo el objetivo de este grupo manejar entre el 70%-80% del de los problemas del usuario antes de concluir en la necesidad de escalar la incidencia a un nivel superior.
d. Soporte Técnico Nivel 2:(*El soporte de nivel dos en la entidad, será desempeñado exclusivamente por un funcionario de planta, el cual dispondrá del conocimiento necesario para esta actividad*), En caso de ser necesario la atención más especializada se canalizada a nuestro pool de soporte especializado, donde será atendido por un especialista con más experiencia en el tema.
e. Soporte Técnico Nivel 3: En caso de que el problema no pueda ser resuelto por el pool de nivel 2, Una vez analizado el caso y según se requiera, se debe proceder con el escalamiento al proveedor para dar solución a la solicitud.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, busca proteger los procesos críticos contra fallas mayores en los sistemas de información o contra desastres y debe garantizar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una eventual contingencia.

La continuidad del negocio deberá ser gestionada por Alta Dirección, que será la responsable de velar por la implantación de las medidas relativas a ésta. Ver TIC-PRO-03 CONTINUIDAD DEL NEGOCIO

15. ACUERDOS DE CONFIDENCIALIDAD

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo con el formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

16. CONCIENCIACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

a. El Club Ecopetrol Bogotá debe mantener un programa anual de concientización y capacitación para todos los funcionarios y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.
b. Todos los funcionarios y contratistas al servicio del Club Ecopetrol Bogotá, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

17. SANCIONES PREVISTAS POR INCUMPLIMIENTO

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto en el manual de ética, código de buen gobierno corporativo, reglamento interno de trabajo, leyes civiles y penales acorde al tipo de vinculación con la Corporación.

18. CONTROL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN
2	09/07/2026	
1	26/10/2023	Creación de lineamiento

19. CONTROL DE FIRMAS

ELABORADO POR:	REVISADO POR:	APROBADO POR:
	Kevin Rodriguez	Lyda M. Zabaleta R.
Técnico Sistemas Juan Camilo Garavito	Técnico Sistemas Kevin Rodríguez	Gerente General Lyda Milena Zabaleta R.
VoBo DE HSEQ	ENTRA EN VIGENCIA A PARTIR DEL 1 de agosto 2026	