TABLA DE CONTENIDO

INDICE DE TABLAS

1. OBJETIVO

Definir los lineamientos de seguridad para sistemas de información y servicios informáticos en ECOPETROL S.A. con el fin de propiciar la disponibilidad, integridad y confidencialidad de la información.

2. DESARROLLO

2.1 ALCANCE

Estos lineamientos aplican a los administradores de la infraestructura de tecnología y a todos los funcionarios y contratistas usuarios de los servicios informáticos de Ecopetrol S.A.

2.2 SEGURIDAD LÓGICA

2.2.a Autenticación de usuarios

Tipos de Cuentas:

Cuentas de servicio: Son las cuentas utilizadas para proporcionar una concesión de permisos para ejecutar un proceso en el sistema sin intervención Humana, por ejemplo: una cuenta para correr una tarea programada, levantar o iniciar un servicio, realizar la conexión o integración a un sistema.

Cuenta Privilegiada: Es toda cuenta destinada a la gestión y administración de los recursos tecnológicos de ECOPETROL S. A.

Cuentas Estándar: Es toda cuenta de acceso a los recursos de ECOPETROL S.A. restringida y sin privilegios. En este tipo de cuenta se encuentran las "Cuentas de Contratistas" y "Cuentas de los funcionarios de Ecopetrol".

Cuenta de Usuarios Guest: Es toda cuenta con dominio externo que hacen parte del tenant de Ecopetrol con invitados y que poseen acceso a aplicaciones.

a) Para acceder a los servicios informáticos de la organización todo trabajador de ECOPETROL S.A. o de empresa contratista debe tener una cuenta que lo identifique y se encuentre autorizada con el fin de que pueda acceder a la información que requiera para el cumplimiento con sus funciones.

b) En caso de requerir acceso remoto a través de la VPN, los equipos de funcionarios y terceros contratistas que no estén registrados en el directorio activo deben instalar el software cliente de VPN suministrado por Ecopetrol S.A. mediante enlace (URL) del portal aprobado por Ecopetrol. El acceso a la VPN debe cumplir con el doble factor de autenticación 2FA o MFA.

c) Todo trabajador de ECOPETROL S.A. o de empresa contratista que administra recursos en la infraestructura de red de la compañía, debe utilizar las soluciones de seguridad avaladas por

ECOPETROL S.A. para el acceso a los sistemas utilizando cuentas privilegiadas, en caso de que no sea posible debe tener una cuenta privilegiada diferente a la cuenta estándar.

d) Todo trabajador de ECOPETROL S.A. o de empresa contratista que sea responsable de un servicio, debe hacer uso de una cuenta destinada (Cuenta de Servicio) para el despliegue y prestación de este en la red de datos de la compañía. Ninguna cuenta que consume recursos de la red de datos (Cuenta Estándar o Cuenta Funcional) debe tener enrolado o estar atado a un servicio. Añadido a lo anterior el nombre de la cuenta no debe tener indicios del servicio que va a prestar y debe cumplir con las políticas de contraseña establecidas en este documento.

e) Los privilegios requeridos para el acceso a los sistemas de información deben cumplir con lo establecido en el control de revisión de accesos.

f) Toda persona, para hacer uso de los recursos de la red de datos, sistemas de información y servicios informáticos de Ecopetrol, debe tener asignado una cuenta de usuario. Por lo tanto, toda cuenta de acceso a sistemas o servicios informáticos debe tener un responsable, incluyendo las cuentas genéricas.

g) Todo usuario debe autenticarse mediante su cuenta de usuario antes de tener acceso a los recursos informáticos de la red de datos.

h) El nombre de la cuenta de usuario, para usuarios finales, debe tener una longitud mínima de ocho (8) caracteres, para los casos que el sistema de información o recurso informático lo permita.

Para el caso de cuentas de usuario final dentro de la red de ECOPETROL S.A., se debe utilizar la siguiente estructura y no será cambiado durante la existencia de relación laboral sin importar su sede de trabajo:

- **xnnnnnnn** donde:

Tabla 1. Para cuentas de usuario final

- x:	**e** para empleados **c** para contratistas
- nnnnnnn:	Número de registro del empleado que se obtiene del número de personal en la solución SAP al momento de creación en el sistema. Para el caso de los usuarios contratistas se toman los 7 primeros dígitos del documento de identificación (CC, CE, …). Si este número (SAP o documento de identidad) tiene una longitud inferior a 7 dígitos se completará está cantidad adicionando ceros (0) después de la letra e o c.

Ejemplos:

Si el número de personal en SAP del empleado es 289388, su usuario de red será e0289388. Si el contratista tiene cédula 71.234.567, su usuario de red será c7123456.

Si se llega a presentar duplicidad en el registro del empleado debido al antiguo manejo de códigos por distrito (02, 03, …,09), se reemplazará el primer cero después de la letra e por la letra A.

Si se llega a presentar duplicidad del número de cédula por su truncamiento, el último dígito debe ser reemplazado de acuerdo con la siguiente tabla de equivalencias:

1	2	3	4	5	6	7	8	9	0
A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	Z	Y	X	W

Para el caso de las empresas del grupo empresarial que tendrán acceso a los sistemas de información y los servicios de TI de la matriz:

Se establece que para separar los usuarios de las empresas del grupo de los de la matriz se aplicará de la siguiente forma:

La cadena de caracteres se divide en tres segmentos.

Tabla 2. Cadena de caracteres

PRIMER SEGMENTO	SEGUNDO SEGMENTO	TERCER SEGMENTO
E= Empleado C= Contratista / Consultor 1 carácter	Tabla de equivalencia para País y sociedad 2 caracteres	Ficho o 5 últimos dígitos de la cédula de ciudadanía 5 caracteres

Para el segundo segmento se define la siguiente tabla con la siguiente secuencia: Primera letra la inicial del país de la sociedad, el segundo carácter número consecutivo (hexadecimal) de la sociedad en este país; por ejemplo:

Tabla 3. Definición para el segundo segmento

SIGLA	País	Nombre de la Sociedad
C1	Colombia	ODL-Oleoducto Bicentenario de Colombia S.A.S.
C2	Colombia	Reficar - Refinería de Cartagena S.A.
C3	Colombia	Bionergy Ltda.
C4	Colombia	Esenttia (Propilco y Comai)
C5	Colombia	Hocol Petroleum Limited S.A.
C6	Colombia	Ecopetrol Costa Afuera Colombia S.A.S
C7	Colombia	Equion Energía Limited
C8	Colombia	OCENSA – Oleoducto Central S.A.
C9	Colombia	Cenit Transporte y Logística de Hidrocarburos S.A.
CA	Colombia	Oleoducto de Colombia S.A.
CB	Colombia	Ecopetrol Energía S.A.S. E.S.P
B1	Brasil	ECOPETROL DO BRASIL
P1	Peru	Ecopetrol del Peru
U1	U.S.A.	ECOPETROL AMERICAS INC
E1	España	Ecopetrol Global Energy

Ejemplos

- Usuario: **Oswaldo Montes** - Empleado de REFICAR sin cuenta en ECOPETROL

Tabla 4. Ejemplo 1 de asignación de usuario

PRIMER SEGMENTO	SEGUNDO SEGMENTO	TERCER SEGMENTO
E	C2	43319
1 carácter	2 caracteres	5 caracteres

- Usuario: **Emerson Viera** - Contratista de ECOPETROL DO BRASIL

Tabla 5. Ejemplo 2 de asignación de usuario

PRIMER SEGMENTO	SEGUNDO SEGMENTO	TERCER SEGMENTO
C	B1	99142
1 carácter	2 caracteres	5 caracteres

i) Para aquellos códigos que presenten duplicidad, en el numeral 2.2.a Autenticación de Usuarios se establece cómo reemplazar el último digito por una letra.

j) Para los empleados de Ecopetrol, con usuario asignado en ECP, que se encuentran en misión en una de las filiales se debe conservar su código original de modo que conserve servicios de TI que recibe mediante este usuario. Se tiene en cuenta que la persona no pierda servicios que hoy tiene o los datos históricos que conserva (Ej. Directorio activo, Outlook, accesos, privilegios de autorizador).

k) El nombre de las cuentas de servicio y cuentas genéricas no debe tener ningún tipo de relación con ECOPETROL ni el servicio que va a prestar o al que se va a sujetar.

l) En el evento que un empleado de una filial o de una empresa contratista pase al servicio de Ecopetrol, se debe crear una cuenta nueva de Ecopetrol como un nuevo trabajador.

m) Toda solicitud de acceso a los sistemas de información o recursos de tecnología deberá hacerse a través del mecanismo definido para ello vigente al momento de la solicitud y cumpliendo con los requisitos y autorizaciones establecidas.

n) Para los accesos de los servicios disponibles en plataforma Office 365, todos los usuarios deberán contar con el Múltiple Factor de Autenticación (MFA).

2.2.b Creación de cuentas de usuarios Guest

Ecopetrol gestiona (creación, actualización y eliminación) los accesos de usuarios guest correspondientes para que personas externas a la organización puedan unirse a los servicios de trabajo colaborativo y aplicaciones, asignándoles cuentas de invitados.

Para la creación de cuentas de usuarios guest, se debe realizar la solicitud diligenciando el formato "Solicitud sobre cuenta de usuario" el cual debe ir firmado por el usuario solicitante (usuario externo) y el profesional de activos, y debe ser enviado por correo electrónico al líder funcional quien realiza la verificación de requisitos y análisis de segregación de funciones para validar si se encuentran conflictos al respecto. Una vez realizadas las respectivas validaciones, el líder funcional envía al administrador del sistema para que cree el usuario en el sistema (Azure Active Directory), al usuario solicitante le llega una invitación, esta debe confirmarse para que se le asigne el rol requerido.

Una vez finalizado este proceso se le comunica al usuario solicitante por correo electrónico sobre la

creación de su cuenta de usuario guest, incluyendo un link para que verifique su funcionamiento y proceder a la asociación de contratos solicitados.

- Actualización / modificación de cuentas de usuario Guest

La actualización de las cuentas de usuario guest se realiza por medio del formato (solicitud sobre cuenta de usuario) marcando en la casilla modificar, se seleccionan los roles a cambiar, debe estar firmado por el usuario solicitante y el profesional de activos y debe ser enviando por medio de correo electrónico al líder funcional quien realiza la verificación de requisitos y análisis de segregación de funciones para validar si se encuentran conflictos al respecto. Las modificaciones solicitadas.
Una vez realizadas las respectivas validaciones, el líder funcional envía al administrador del sistema para que realice la modificación del usuario en el sistema (Azure Active Directory), luego el usuario solicitante debe validar el respectivo funcionamiento.

- Deshabilitación y/o eliminación de cuentas de usuarios guest

Toda cuenta de usuario guest, asociada a externos y/o proveedores de ECOPETROL S.A. se deshabilitará luego de 30 días de inactividad.

Toda cuenta de usuario guest, asociada a externos y/o proveedores de ECOPETROL S.A. deshabilitada, se eliminará luego de 30 días si el usuario o el responsable no solicita su reactivación.

2.2.c Gestión de contraseñas

La autenticación de usuarios se hace con el uso de una contraseña, por lo tanto, la adecuada gestión de las contraseñas es un aspecto importante para proteger el acceso a los sistemas de información. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de la información y servicios de Ecopetrol. Por lo anterior se indican los siguientes lineamientos:

a) No se deben utilizar contraseñas por defecto. La gestión de cambio de contraseña de todas las cuentas es obligatoria para todos los recursos, una vez asignada la cuenta se debe hacer el primer cambio de contraseña, estas deben cumplir con los tiempos en los cambios de contraseña según el tipo de cuenta (Cuentas de Administración, Cuentas de Servicio, Cuentas Funcionales y Cuentas Estándar) en caso de no poder generar este cambio se debe presentar la Justificación y Aprobación por parte del Coordinador de Plataformas, Ciberseguridad y Ciberdefensa.

   Se deben cambiar las contraseñas que traen los equipos y sistemas por defecto. Con esta medida evitamos el acceso no permitido, que sería posible si dejamos la contraseña por defecto por ser estas conocidas o que pueden encontrarse fácilmente en internet.

b) No se deben compartir las contraseñas, estas deben ser de uso personal. Las cuentas y credenciales son de uso personal e intransferible y exclusivo para el acceso del titular. Queda terminantemente prohibido compartir estas con otros usuarios o terceros, en caso de que este evento sea confirmado se considerará como un **INCIDENTE DE SEGURIDAD,** notificación a jefe

inmediato, con incidencia en control disciplinario de Ecopetrol.

Se debe asegurar lo siguiente:

c) No escribirlas en lugares visibles o de acceso a otras personas.
d) No escribir las contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.

- Las contraseñas deben de ser robustas. Para que las contraseñas sean fuertes, difíciles de deducir o calcular, se deben cumplir las siguientes directrices para los casos que el sistema de información o recurso informático lo permita:

  - Deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos), para los casos que el sistema de información o recurso informático lo permita.
  - No deben contener los siguientes tipos de palabras:

    - Palabras sencillas en cualquier idioma (palabras de diccionarios)
    - Nombres propios, fechas, lugares o datos de carácter personal.
    - Palabras que estén formadas por caracteres próximos en el teclado; o palabras excesivamente cortas.
    - Aplicar la creación de contraseñas mediante una frase (puede ser cualquier palabra, frase, cualquier conjunto de letras, o incluso una oración) con sus respectivos espacios.

  - No utilizar claves formadas únicamente por elementos o palabras que puedan ser públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento).
  - Se deben establecer contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas.

- No se debe utilizar la misma contraseña para servicios diferentes. Tampoco se deben utilizar las mismas contraseñas para uso profesional y uso personal

- Se deben cambiar las contraseñas periódicamente. Según el tipo de cuenta y el tiempo establecido para cada una de esta, es de carácter obligatorio el cambio de contraseña para todas las cuentas como se indica a continuación:

  Cuentas de Servicio: Todas las Cuentas de Servicio deben cambiar su contraseña por lo menos una vez cada 180 días.

  Cuentas de Administración**:** Todas las Cuentas de administración deben tener MFA, cambiar su contraseña cada 30 días, debe tener una longitud de 12 caracteres y que el desbloqueo no sea automático.

  Para las cuentas con privilegios a nivel del dominio, Administrators, Domain Admins, Enterprise Admin y Schema Admin el cambio del password se hará cada 30 días, para este tipo de cuentas el password debe tener una longitud mínima de 12 caracteres y que el desbloqueo no sea

automático, este se debe solicitar a la mesa de ayuda o con el administrador del servicio según aplique.

Cuentas Privilegiadas: Todas las Cuentas Privilegiadas deben tener MFA y cambiar su contraseña cada 120 días, para este tipo de cuentas el password debe tener una longitud mínima de 12 caracteres y que el desbloqueo no sea automático, este se debe solicitar a la mesa de ayuda.

Cuentas Estándar: Todas las Cuentas Estándar deben tener MFA, cambiar su contraseña cada 180 días, debe tener una longitud mínima de 12 caracteres y que el desbloqueo no sea automático, este se debe solicitar a la mesa de ayuda.

Cuentas Genéricas: Todas las Cuentas Genéricas deben tener MFA si aplica y cambiar su contraseña cada 120 días, para este tipo de cuentas el password debe tener una longitud mínima de 12 caracteres.

- Si un usuario y sus credenciales son custodiados por Keyvault sus contraseñas no requieren cambio. Aplica para los casos que el sistema de información o recurso informático lo permita.

- Si el recurso tecnológico se autentica contra el Directorio Activo, le aplican los parámetros de contraseñas del Directorio Activo. Para los recursos tecnológicos que no se autentiquen con el Directorio Activo y manejan su propia base de datos de usuarios para permitir la autenticación, el cambio de las contraseñas se debe aplicar cada 60 días y debe tener una longitud mínima de 12 caracteres y que el desbloqueo debe ser manual. Para los casos que el sistema de información o recurso informático lo permita. El proceso de cambio debe ser notificado al área de Ciberseguridad y Ciberdefensa. En caso de no ejecutar lo establecido en este apartado se considerará un Incidente de Seguridad.

- En caso de requerirse una excepción al punto anterior de esta política, se debe solicitar un análisis de riesgos al correo electrónico a ciberseguridadyaccesos@ecopetrol.com.co en donde se evalúa el caso particular si amerita o no la excepción.

- Sin embargo, los usuarios pueden cambiar su clave cuando lo consideren conveniente y de forma inmediata cuando la contraseña pueda haber sido comprometida.

  Histórico de contraseñas. **NO** deben utilizarse contraseñas que hayan sido usadas con anterioridad, debe ser diferente a las últimas 24. En los sistemas que lo permitan se debe forzar el cumplimiento de esta norma.

- Uso de gestores de contraseñas. Considerar el uso de gestores de contraseñas en aquellos casos en los que se tenga que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo supervisión, que cifre las credenciales e implantar doble factor de autenticación para acceder al mismo.

- En caso de requerirse activar nuevas funcionalidades de autenticaciones como, por ejemplo: biometría digital y PIN, enlazadas a las credenciales del usuario desde el equipo corporativo, estás se incorporarán según necesidad de ECOPETROL.

- Toda cuenta de usuario final asociada a funcionarios o contratistas de ECOPETROL que no se utilice por un período de 60 días, cualquiera que sea el motivo de la falta de uso, debe ser deshabilitada; su habilitación debe ser solicitado por el usuario o realizado por autogestión, si está disponible. Tenga en cuenta que, si un usuario no se conecta a la red de datos de Ecopetrol por lo menos una vez en el periodo indicado, el sistema deshabilitara su cuenta.

- Toda cuenta que supere el tiempo de inactividad se moverá a la unidad organizacional (OU) *Cuentas Deshabilitadas* y se le quitaran todos los privilegios y grupos con los que contaba. En caso de requerirse activar de nuevo la cuenta con los respectivos permisos, estos deben ser solicitados nuevamente a la mesa de servicio con la autorización del director, Líder o dueño de contrato por parte de Ecopetrol.

- Toda cuenta de usuario final asociada a funcionarios o contratistas de ECOPETROL que no sea utilizada o reactivada por un período de 60 días después de que se encuentre en estado "deshabilitado" se debe proceder a ser eliminada, excepto para funcionarios en el sistema SAP-ERP por la funcionalidad existente de Autogestión, en cuyo caso se le retirarán los roles diferentes a Autogestión y la cuenta quedará no interactiva. Aplicará la eliminación de la cuenta cuando se reciba la notificación de la desvinculación del funcionario. Se exceptúan también otros sistemas de información que por su funcionalidad requieran un periodo diferente. El líder funcional realizará seguimiento periódicamente en la actualización y depuración de base de usuarios, de acuerdo con los lineamientos definidos.

- Toda cuenta de usuario final de ECOPETROL S.A. en Directorio Activo debe ser bloqueada automáticamente, después de hasta CUATRO (4) intentos de ingresos consecutivos y fallidos, sin perjuicio de que se permita una configuración más restrictiva en algunos sistemas. El contador de intentos de ingreso se restablecerá a cero después de 30 minutos de un inicio de sesión fallido. Esta norma aplica también a los sistemas de información y a cualquier otro servicio de la red, siempre que sea técnicamente viable en el sistema correspondiente. La reactivación debe ser solicitada de acuerdo con el procedimiento de solicitud de servicios establecido.

- Para los equipos que están registrados en el dominio de Ecopetrol les aplican las políticas de bloqueo de sesión por inactividad desplegada por GPO.

- Para des-habilitaciones de servicios de TI favor remitirse al documento normativo: Procedimiento para la gestión de des-habilitación de servicio de TI.

- Cuando el sistema permita el control de la fecha de vencimiento de los servicios, éste se debe implementar para todos los usuarios. De no permitirlo, es responsabilidad del líder funcional hacer seguimiento, la actualización y depuración de base de usuarios.

- Atributo contraseña no expira. Ninguna cuenta de Ecopetrol, filiales y contratistas (servicio, estándar, funcional o administrativa) **NO** debe tener habilitado el atributo de la contraseña no expira (Never Expired). En caso de requerirse una excepción se debe solicitar un análisis de riesgos al correo electrónico a ciberseguridadyaccesos@ecopetrol.com.co en donde se evalúa el caso particular si amerita o no la excepción

- Atributo contraseña vacía. Ninguna cuenta de Ecopetrol, filiales y contratistas (servicio, estándar, funcional o administrativa) **NO** debe tener habilitado el atributo de contraseña vacía (Password-Not-Required).

2.2.d Control de Acceso

Antes de autorizar un servicio a un usuario, se deben establecer los privilegios que tiene sobre los recursos. En esta acción intervienen el usuario y el funcionario que lo autoriza (funcionario de nivel superior de la dependencia, administrador o gestores en caso de contratistas) y los administradores de los servicios, como proveedores de información relacionada con los posibles permisos de acceso al recurso.

Se debe crear una cuenta de administración independiente para actividades normales de la función, es decir, backups, administración de impresoras, de disco, bloqueo de sesiones, de cuentas, apagado del sistema e instalación de controladores. Ésta, no podrá ser utilizada para actividades diferentes a las preestablecidas.

El administrador del sistema debe crear únicamente los usuarios autorizados, respetando los privilegios asignados.

El acceso a la información depende de la clasificación que el responsable de la información otorgue de acuerdo con el Manual de Seguridad de la Información Las solicitudes de información deben acompañarse por el nivel de autorización explícito, por el funcionario responsable de acuerdo con el mencionado manual.

La circular emitida por la Presidencia de Ecopetrol establece: "Considerando la propiedad de la información de Ecopetrol S.A., las áreas de control y/o de cumplimiento de la empresa tienen la facultad de asegurar, acceder, captar, revisar, tratar, transferir, utilizar o monitorear, toda la información de la empresa". Por lo anterior, funcionarios de las áreas mencionadas, para el ejercicio de sus funciones, podrán solicitar acceso de consulta a los sistemas de información de Ecopetrol y los lideres funcionales o encargados de la asignación del acceso deberán otorgárselo. La solicitud deberá tener la debida aprobación del jefe del área del solicitante.

Todo equipo de cómputo de proveedor o contratista que solicite el ingreso al dominio ECOPETROL S.A. deberá conocer, aceptar y cumplir con el Manual de Seguridad de la Información publicado en OpenText y la presente guía.

Todo equipo de cómputo de proveedor o contratista que requiera conexión a la red de datos debe garantizar que su ingreso no afecte los servicios informáticos, que sus aplicaciones y el sistema operativo se encuentren actualizados, que no tenga instalado software que afecte la seguridad de la información y cuente con un software antimalware debidamente licenciado y con las últimas

actualizaciones. Adicionalmente, todo software instalado debe ser legalmente licenciado y el contratista responde por la normatividad relacionada con derecho de autor. Ecopetrol se reserva el derecho de monitorear el estricto cumplimiento de estas condiciones y de reportar o bloquear, de manera autónoma e inmediata cualquier dispositivo que no cumpla y que implique riesgos para la seguridad y cumplimiento.

2.2.e Copias de Respaldo

Toda la información clasificada o reservada deberá mantenerse almacenada en los servidores corporativos o que cumplan con la normativa de seguridad para servicios en la nube y/o protección de datos personales, indicando los respectivos usuarios y permisos. La disponibilidad de esta información se garantizará de acuerdo con los procedimientos de respaldo existentes.

2.2.f Servidores

El administrador de un sistema o servicio informático debe, con la frecuencia definida en la política de Backup y recuperación de información, hacer la copia de seguridad protegida contra escritura y verificar periódicamente su contenido, el cual debe contemplar lo siguiente:

- El sistema operativo junto con las tablas relacionadas (datos de configuración).
- Software de red
- Compiladores
- Software de aplicación
- Archivos de seguridad
- Librerías de programas
- Archivos de datos

Los administradores de backup deben asegurar que la información a respaldar, pactada en las actas de backup con los negocios o responsables de las aplicaciones y servicios informáticos, se guarde y esté disponible en el momento que se requiera.

Una copia de archivos de respaldo debe residir en una cintoteca o centro alterno de almacenamiento, ubicado fuera de los centros de cómputo de ECOPETROL S.A., que cuente con una bóveda o bodega adecuada para tal fin. Se deben mantener los controles necesarios para conocer el estado de cada copia de respaldo y su ubicación.

Los sitios internos que ECOPETROL S.A. disponga como bodegas o centros de almacenamiento de registros vitales, documentación y/o copias de respaldo, deben cumplir con los requerimientos físicos, logísticos y de seguridad adecuados para tal fin. Debe existir una copia de respaldo de la documentación de las aplicaciones, ubicada en un sitio externo a las instalaciones donde se encuentra la documentación original.

Dentro de ECOPETROL S.A., se debe realizar un backup total del sistema, antes de efectuar cualquier actualización de éste.

Se deben implantar procedimientos para preparar, almacenar y probar periódicamente la integridad de las copias de seguridad y de toda la información necesaria para restaurar el sistema a una operación normal.

2.2.g Equipos Corporativos

Se entiende por equipos corporativos a los computadores y dispositivos móviles aprovisionados por Ecopetrol S.A que cumplen con los estándares de seguridad determinados por la compañía para la protección y seguridad de la información, los cuales son asignados a los colaboradores para gestionar, acceder, tratar, transferir, utilizar la información que sea generada, administrada, enviada, recibida y/o almacenada en dichos equipos, para fines institucionales.

Todo usuario es responsable de acatar, implementar y cumplir las medidas vigentes y sobrevinientes relacionadas con la protección de los equipos a su cargo según lo estipulado en el código de ética y conducta de Ecopetrol: *"Todo trabajador tiene la responsabilidad de proteger la información y los recursos tecnológicos que le entregó Ecopetrol (direcciones electrónicas, acceso a internet, computadores, dispositivos móviles, etc.), los cuales están destinados de forma única y exclusiva al desempeño de sus funciones y/o tareas, y no deben ser usados para otros fines, conforme con los reglamentos internos"*. El usuario deberá participar activamente para asegurar el cumplimiento de los procedimientos de actualización, monitoreo y control que sobre los equipos asignados ejecuta la organización, así mismo debe hacer la utilización únicamente de software autorizado para el uso de este.

Cada usuario es responsable de hacer copias de respaldo sobre aquella información que no se encuentre almacenada en los servidores corporativos, por lo tanto, debe asegurar la sincronización de su información en OneDrive empresarial desde el equipo corporativo.

2.2.h Medidas de Seguridad Mínimas para los Sistemas y Servicios Informáticos

Todo sistema nuevo o actualización de sistema debe contar con el análisis de seguridad correspondiente, antes de ingresar a producción, en donde se verifique que todas las posibles vulnerabilidades existentes tanto en el sistema operativo como en el aplicativo y en la base de datos son superadas y se encuentran debidamente cerradas. Los sistemas de información clasificados como priorizados deben cumplir con los controles clave, exigidos por Ecopetrol S.A.

En la instalación y configuración de infraestructura, se deben aplicar las listas de "endurecimiento" o de seguridad definidas para cada plataforma

2.2.i Aspectos de Seguridad para Compartir Directorios y/o Archivos

El manejo compartido de información mediante directorios y/o archivos debe seguir las normas de clasificación de la información contenidas en el Manual de Seguridad de la Información y usar las herramientas oficiales para compartir archivos como el OneDrive o SharePoint.

Cuando un usuario comparta directorios y/o archivos de datos desde el computador bajo su custodia

o desde su Sitio de OneDrive o SharePoint, debe establecer esquemas de seguridad de acceso considerando como mínimo los siguientes aspectos:

- Definición y control de usuarios autorizados al archivo o al directorio.
- Activación de permisos de lectura, escritura y/o control total sobre el archivo o directorio, según se requiera.
- Revisión periódica de la vigencia de los permisos.

Cuando se requiera compartir información a través de un directorio en un servidor de la red de datos, el usuario responsable debe solicitar a Service Desk, la creación del directorio, así como la asignación de los permisos de acceso que cada usuario autorizado tendrá sobre el directorio y/o sus archivos. El contenido de las carpetas será responsabilidad del dueño de las mismas.
De igual manera, será responsabilidad de los dueños de las carpetas o directorios, realizar la depuración de manera periódica de los usuarios y permisos asignados.

2.2.j Seguridad en Medios de Almacenamiento Externos

No está permitido el uso de dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) para almacenamiento o transporte de información. La Información CLASIFICADA y/o RESERVADA se debe gestionar en los sistemas de almacenamiento corporativos y ser compartida únicamente en los medios de almacenamiento seguros definidos por la organización.

Por razones de seguridad, se des-habilitarán las interfaces USB para almacenamiento de los equipos corporativos y se desactivará la opción de autoarranque para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles sean conectados. En caso de ser necesaria su habilitación, deberá solicitarse a Service Desk con copia a su Jefe inmediato, la respectiva activación indicando la excepción según aplique:

- Llaves/Tokens tipo USB para aplicaciones especializadas
- Pockets/IED/Equipos de campo que usen el puerto USB para descarga de información
- Otra situación avalada por el Jefe inmediato, que impacte las Operaciones de la Empresa

Alternativas a los medios de almacenamiento extraíble. Para evitar del uso de estos dispositivos, deben utilizarse las siguientes alternativas:

- Repositorios comunes para el intercambio de información, como SharePoint Online.
- Servicios de almacenamiento en la nube autorizados por ECOPETROL, como OneDrive.

3. CONTINGENCIAS

N/A

RELACIÓN DE VERSIONES

Documento Anterior			
Versión	**Fecha dd/mm/aaaa**	**Código y Título del Documento**	**Cambios**
1	12/06/2020	SGY-G-002	Cambio de código por cambio de sistema de gestión. Actualización de la normativa de seguridad para las contraseñas. Establecimiento de normativa en seguridad en medios de almacenamiento externo. Eliminación de la codificación de las normas referidas en el documento; teniendo en cuenta se actualizarán sus códigos.
2	23/10/2020	SGY-G-002	*Se incluye el valor del histórico de contraseñas *Se incluye el valor del contador de intentos fallidos para bloquear automáticamente una cuenta de usuario final. * Se incluye la aplicabilidad de los parámetros de contraseñas para el Directorio Activo y de aplicaciones.
3	28/09/2021	SGY-G-002	• En el numeral 2.2.a: se incluyen indicaciones para conexión remota mediante VPN y se aclara que para conexión se aplica el MFA. • En el numeral 2.2.b : 1. para los cambios de contraseñas se incluyen las credenciales custodiadas por Keyvault. 2. Se incluyen características de tiempos y longitud del password en cuentas Domains Admins y KDC. 3.Se incluye como responsabilidad del líder funcional el seguimiento periódico den la actualización y depuración de base de datos de usuarios para cuentas

			de usuario final. • En el numeral 2.2.d:se cambia el título "Equipos personales" por "Equipos Corporativos" y se amplía el contexto del uso y responsabilidad de estos.
4	19/10/2022	SGY-G-002	• Se actualizó la redacción del documento. • En el numeral 2.2.a Autenticación de usuarios, se actualizan las definiciones de tipos de cuentas, accesos remotos a través de VPN, autenticación MFA. • Adición del numeral 2.2.b Creación de cuentas de usuarios Guest, que contiene la actualización/modificación, des habilitación y eliminación de cuentas de usuarios Guest. • 2.2.c En el numeral Gestión de contraseñas, se actualizó el apartado Las contraseñas deben ser robustas, contraseñas por defecto, contraseñas de uso personal, cambios periódicos de contraseñas, parámetros de contraseñas en directorio activo, históricos de contraseñas, tiempo de inactividad en cuentas de usuarios, mejora en la redacción de apartado bloqueo de escritorio por inactividad y atributos de contraseñas. • Forma general de la redacción.

Documento Nuevo		
Versión	**Fecha dd/mm/aaaa**	**Cambios**
N/A	N/A	N/A

Para mayor información dirigirse a:

Elaboró: Erica Alexandra Reina
Teléfono:42299
Buzón: erica.reina@ecopetrol.com.co
Dependencia: Gerencia Ciberseguridad y Ciberdefensa

Revisado electrónicamente por:	Aprobado electrónicamente por:
JUAN SEBASTIAN ROJAS SALAMANCA Coordinador de Ciberseguridad **Cédula de Ciudadanía No. 1.069.724.583** Vicepresidencia De Ciencia Tecnología e Innovación	**EDGARDO ALFONSO ARRIETA ARTETA** Gerente Ciberseguridad y Ciberdefensa **Cédula de Ciudadanía No. 77.195.540** Vicepresidencia De Ciencia Tecnología e Innovación

Documento firmado electrónicamente, de acuerdo con lo establecido en el Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Para verificar el cumplimiento de este mecanismo, el sistema genera un reporte electrónico que evidencia la trazabilidad de las acciones de revisión y aprobación por los responsables. Si requiere verificar esta información, solicite dicho reporte a Service Desk.