
combuscol
100% COMBUSTIBLES DE COLOMBIA
POLÍTICA DE SEGURIDAD
REGLAMENTO TECNOLOGÍA
DEPARTAMENTO DE TECNOLOGÍA
COMBUSTIBLES DE COLOMBIA S.A.

Contenido

1. Objetivos

El objetivo de la Política de Seguridad Informática consiste en establecer unos criterios, directrices y estrategias que le permitan **COMBUSTIBLES DE COLOMBIA S.A**. proteger su información, así como la tecnología para el procesamiento y administración de la misma.

La Política de Seguridad Informática proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades del sistema.

El propósito de estructurar Políticas de Seguridad Informática es, por tanto, garantizar que los riesgos para la Seguridad Informática sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad informática consiste en garantizar la confidencialidad, Integridad y Disponibilidad de la información.

Al aclarar las responsabilidades de los usuarios y las medidas que deben adoptar para proteger la información y los sistemas informáticos, **COMBUSTIBLES DE COLOMBIA S.A**. evita pérdidas graves o divulgación no autorizada.

Este documento formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad informática y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales **COMBUSTIBLES DE COLOMBIA S.A**. establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la organización, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la empresa.

El presente documento define los lineamientos que debe seguir la **COMBUSTIBLES DE COLOMBIA S.A.** con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

2. Alcance

2.1. Los Empleados

La seguridad informática es un esfuerzo en equipo. Esto requiere de la participación y el esfuerzo de todos los miembros de la organización que trabajan con los sistemas de información.

Así, cada empleado deberá comprometerse en el cumplimiento de los requisitos de la Política de Seguridad Informática y de los documentos asociados a la misma.

2.2. Los Sistemas (Hardware y Software)

Esta Política aplica para todos los computadores, redes, aplicaciones y sistemas operativos que son propiedad o son operados por **COMBUSTIBLES DE COLOMBIA S.A**. La Política cubre únicamente la información manejada por los computadores y las redes de la organización.

2.3. Contratistas

Se definen como contratistas a aquellas personas que han suscrito un contrato con **COMBUSTIBLES DE COLOMBIA S.A.**

- Colaboradores por Outsourcing: son aquellas personas que laboran en la empresa y tienen contrato con empresas de suministro de servicios y que dependen de ellos.
- Personas naturales que prestan servicios independientes a la empresa.
- Proveedores de recursos informáticos.

2.4. Entidades de Control

- Revisoría Fiscal
- Auditoría Interna

2.5 Otras Entidades

- DIAN

3. Responsabilidad

3.1.1. Direcciones o Áreas responsables de la Seguridad Informática

Directores, jefes de área, Coordinadores y Administradores de los diferentes centros de operaciones son responsables de cumplir la política de seguridad de la información, así como del cumplimiento de dicha política por parte de su equipo de trabajo.

La política de seguridad de la información es de aplicación obligatoria para todo el personal, cualquiera sea el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe.

3.1.2. Junta Directiva y Gerencia

La **Junta Directiva** y la **Gerencia** de la compañía aprueban esta política y son responsables de la autorización de sus modificaciones.

3.1.3. Comité de Riesgos

La seguridad de la información es una responsabilidad compartida por toda la compañía, es por esto que se crea el comité de riesgos el cual está integrado por representantes de las diferentes áreas de la compañía, dentro de este comité el jefe de Tecnología cumple el papel de coordinador y es el encargado de impulsar la implementación de la presente política.

3.1.4. Tabla 1 Conformación del comité de Riesgos

AREAS
Gerente General
Director Administrativo y Financiero
Director Comercial y Operativo
Jefe de Tecnología

- Revisar y proponer a la Junta Directiva de **COMBUSTIBLES DE COLOMBIA S.A**. y a la Gerencia para su aprobación la política y las funciones generales en materia de seguridad de la información, esta actividad se realizará anualmente en el mes de enero.

- Conocer, supervisar, investigar y monitorear los incidentes relativos a la seguridad. Se realizará una evaluación anual en el mes de enero para verificar la información recopilada.

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios. Actividad que deberá ser realizada por cada proyecto que sea implementado, al igual que debe quedar documentado.

4. Seguridad Informática

La seguridad informática y manejo de datos lleva a la aplicación de las técnicas para proteger, preservar la información y los distintos recursos informáticos de la Compañía. La política de seguridad informática y manejo de datos **es la reunión de normas, reglas, procedimientos y prácticas que ordenan la protección de la información frente a la pérdida de confidencialidad, integridad o disponibilidad**, bien sea en forma accidental como intencionada, asegurando la conservación y uso adecuado de los recursos informáticos de la Compañía. Cada empleado o

contratista con acceso a información sistematizada y aplicaciones de la compañía es responsable por la conservación de la misma, garantizando su disponibilidad, integridad y confidencialidad. **COMBUSTIBLES DE COLOMBIA S.A.** se encarga de proteger la información almacenada en el centro de datos, salvaguardando la información de los siguientes servicios de la Compañía **Enterprise**, **IntegraWeb**, **Portal Administrativo**, **Sistema UNO** (Información anterior al 2013) y CRM. En relación a CCTV, no se contará con copia de la misma, dado que los tamaños de las imágenes son muy grandes y los costos de almacenamiento costosos, sin embargo, se cuenta con almacenamiento de mínimo 15 días por estación en el NVR y/o DVR dispositivos que se encuentra en la misma estación de servicio, por último, el sistema BIOMETRICO será salvaguardado cada 2 meses. La información almacenada en el computador de los usuarios es responsabilidad del usuario. Es importante mencionar que todos y cada uno de los funcionarios tienen la obligación de almacenar en la nube su información, los funcionarios de **COMBUSTIBLES DE COLOMBIA S.A.** pueden crear y gestionar dicho almacenamiento utilizando **Google Drive**.

El empleado o contratista es el único responsable por el resguardo de la información ubicada en repositorios y aplicaciones diferentes a la definida y autorizada por la compañía. Para los funcionarios que por algún motivo deban almacenar información en repositorios diferentes a la nube deben asegurarse de hacer una copia periódica en la nube de dicha información y es responsable por la pérdida de la misma. En el evento de mal manejo de la información interna o externa por parte del usuario, por extravío o por divulgación a terceros, se entiende vulnerado el deber de cumplir con las obligaciones concretas del puesto de trabajo, de conformidad a las reglas de buena fe y diligencia, por ende, por incumplida la cláusula u obligación de confidencialidad con sus respectivas consecuencias legales y penales.

5. Controles para la administración de la seguridad

5.1 Uso de los sistemas y equipos de cómputo

La Compañía tiene regla de renuncia (Disclaimer), que debe utilizarse al inicio de sesión en los equipos de cómputo.

"¡Advertencia!

- *Usted se dispone a usar un equipo de propiedad de COMBUSTIBLES DE COLOMBIA S.A. Este sistema (hardware, software y periféricos), así como la información en él y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento.*
- *Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan según lo determinado con la política de seguridad de la información."*
- *Este equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.*
- *En caso de presentar una falla física o lógica se deberá notificar al área de Tecnología y en el caso de ser requerido enviar el equipo para su revisión y/o reparación.*
- *En ningún caso el usuario intentará reparar el equipo o diagnosticarlo, únicamente informar de la posible falla.*
- *Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales, en el exterior de todos los equipos se respetará la imagen física de empaque.*
- *Cada usuario es responsable del cuidado de su herramienta de trabajo Por lo que se recomienda limpiar continuamente el equipo externamente,*
- *El usuario será el único responsable del equipo de cómputo, así como de la información contenida en el mismo. Al aceptar, el usuario se compromete dar cumplimiento con lo establecido para el manejo del equipo."*

5.2 Entrega de computadores a usuarios.

La entrega de este activo es realizada por el equipo de tecnología al usuario, para ello se utiliza el siguiente formato:

combuscol	COMBUSTIBLES DE COLOMBIA S. A ACTA DE ENTREGA	Código: 19-AT-05-16 Versión: 01 Página 1 de 2

Proceso Tecnología	
Procedimiento:	Entrega equipos de computo
Funcionario que recibe:	
Funcionario que entrega:	
Ciudad /Fecha:	

Adjunto a la presente se le hace entrega del siguiente equipo:

DATOS DEL EQUIPO	
Tipo	DESKTOP
Fabricante	DELL
Modelo	Vostro 3500
Número de serie	FC7BCL1
Sistema Operativo	Windows 7 Professional
Office	Office Home and Bussines 2013
Antivirus	Symantec Endpoint Protection Versión 12.7

Me comprometo a cuidar y mantener en buen estado la dotación tecnológica brindada por la empresa COMBUSTIBLES DE COLOMBIA S.A. para el cumplimiento de las funciones respectivas a mi cargo.

Las partes que suscriben el presente documento aceptan las siguientes: CONDICIONES ESPECIALES:

1. Declaro conocer que el equipo en cuestión es de propiedad de COMBUSTIBLES DE COLOMBIA S.A. y me es entregado para uso personal e intransferible para realizar exclusivamente las actividades propias del cargo que desempeño y dentro del ámbito laboral. Un uso diferente a esta herramienta de trabajo, se encuentra tipificado en el contrato de trabajo como prohibición y su violación es considerada como falta grave del Contrato de trabajo me comprometo a NO realizar ninguna instalación al equipo sin previa autorización y licenciamiento por el área de Tecnología.

2. Declaro conocer que la información que se grabe o procese en este equipo también es de propiedad exclusiva de COMBUSTIBLES DE COLOMBIA S.A. y me comprometo a no copiarla, suministrarla, transferirla o extraerla para usos no autorizados. El incumplimiento de este compromiso, se encuentra tipificado en el contrato de trabajo como prohibición y su violación es considerada como falta grave del contrato de trabajo. En caso de daño atribuible al fabricante (por garantía) informaré directamente al área de Tecnología para realizar el trámite ante la entidad encargada para la respectiva garantía y no ejecutaré ningún procedimiento en el equipo ni lo llevaré a ningún lugar para ser reparado.

Ilustración 1

3. En caso de terminación del contrato de trabajo o entrega de una nueva dotación, me comprometo a hacer la devolución de forma inmediata ante el Área de Tecnología. Cuando se trate de terminación de contrato, me comprometo a hacer la devolución del equipo con la información recibida y procesada durante el tiempo de tenencia del presente equipo y/o la procesada en equipos anteriores y transferida a este equipo.

FIRMO EN SEÑAL DE ACEPTACION DE LAS CONDICIONES ESPECIFICADAS EN EL PRESENTE DOCUMENTO DE ENTREGA DE EQUIPO DE COMPUTO ASIGNADOS POR LA EMPRESA COMBUSTIBLES DE COLOMBIA S.A. y Me comprometo a cuidar y mantener en buen estado la dotación tecnológica brindada por la empresa COMBUSTIBLES DE COLOMBIA S.A. para el cumplimiento de las funciones respectivas a mi cargo.

Firma de entregado

C.C

Firma de recibido

C.C

Atentamente,

Miguel Ángel Cano Varela
Jefe de Tecnología
COMBUSTIBLES DE COLOMBIA S.A.

5.3 Correo Electrónico

La Compañía, como muestra de respeto por los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la

Compañía; en consecuencia, el jefe de área podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón del correo asignado.

Las comunicaciones por correo electrónico entre la empresa y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la Organización., ni para trasmitir cualquier otro tipo de información del negocio.

A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, está se les asignará una vez vinculados. Los jefes de área son responsables de informar a Tecnología, las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de colaboradores para la suspensión de este servicio.

Esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la Compañía, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez, se produzca la desvinculación de la persona, la cuenta será dada de baja y el almacenamiento del buzón será trasladado a una cuenta que sea previamente definida por la directora operativa y comercial o la directora administrativa y financiera, según corresponda.

El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.

La organización tiene regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes. Para evitar reclamaciones legales todos los usuarios de correo de la empresa tienen que hacer pública la renuncia de responsabilidad legal por el envío de información. El disclaimer aprobado es:

La información contenida en este mensaje y sus archivos anexos están dirigidos exclusivamente a su destinatario, pudiendo contener información confidencial sometida a secreto profesional. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente, acto seguido borre este mensaje, pues su uso (reproducción y distribución) sin la autorización expresa de Combustibles de Colombia S.A no está permitida y acarreará las sanciones y medidas legales a que haya lugar. De acuerdo con la Ley Estatutaria 1581 de 2012 de Protección de Datos y con el Decreto 1377 de 2013, el Titular presta su consentimiento para que sus datos, facilitados voluntariamente, pasen a formar parte de una base de datos, cuyo responsable es Combustibles de Colombia S.A, cuyas finalidades son la gestión administrativa, operativa, y envío de comunicaciones comerciales sobre nuestros productos y/o servicios. Puede usted ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre sus datos, mediante escrito dirigido a Combustibles de Colombia S.A a la dirección de correo electrónico servicioalcliente@combuscol.com *y* protecciondedatos@combuscol.com*, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a la Cra 11 # 71-73 en Bogotá. La empresa no se hace responsable por la presencia de virus o malware en este mensaje o en sus anexos, así como tampoco por los daños que en sus equipos, programas e información se puedan presentar.*

El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la Organización, el usuario se comprometa a:

- ✓ Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.

- ✓ El colaborador titular del correo o cuenta asignada por la Organización, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias a su cargo o de las investigaciones que tenga asignadas; las únicas áreas autorizadas para el envío de correos masivos son la Dirección Comercial y Operativa; otros envíos de información masiva, deben ser aprobadas por Tecnología.

- ✓ Si, el colaborador desea cambiar su imagen de perfil (foto) del correo electrónico, deberá tomar una foto adecuada, sin emoticones y con buena presentación personal (hombres con corbata y mujeres con vestuario formal).

- ✓ El uso del correo electrónico en cabeza de la Organización deberá ser usado solamente para fines propios a la organización. En su uso el colaborador actuará siempre con respecto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, instituciones o realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas religiosas, propagandas entre otros.

- ✓ La Compañía, se abstiene de enviar o recibir los mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualquier mensaje que contenga duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.

- ✓ Los colaboradores de la Compañía se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes SPAM (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticos o normas institucionales.

- ✓ Evitar el envío desde su buzón de elementos (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias

(crackers), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.

- ✓ Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencias de espacio disponible. Estas advertencias se realizan varias veces, en caso que tenga dudas sobre la información, debe solicitar soporte al área de Tecnología.

- ✓ Utilizar la cuenta de correo electrónico corporativa para fines laborales, de investigación y los estrictamente relacionados con las actividades propias de su trabajo. Los colaboradores deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la empresa, la cuenta de correo electrónico no deberá ser usada para cuentas en redes sociales, páginas de compra, venta y otros fines ajenos a la actividad de la compañía.

- ✓ Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa.

- ✓ Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.

- ✓ Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando.

- ✓ En lo posible, es necesario evitar letras mayúsculas, especialmente en el campo de “Asunto:”, al igual que el uso excesivo de signos de exclamación (&,%,$,#,?,!,¡,¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado o spam, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.

5.4 Navegación en Internet

El uso de internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y debe ser utilizado por el colaborador para realizar las funciones establecidas para su cargo, por lo cual la compañía definió los siguientes parámetros para su uso:

- ✓ El colaborador debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.

- ✓ La descarga de música y vídeos no es una práctica permitida.

- ✓ Escuchar música en línea no es una práctica permitida.

- ✓ Evitar el uso de servicios descarga de archivos como: Emule, LimeWare, Morpheus, GNUtella, Atube Catcher o similares.

- ✓ La sala de vídeo conferencia de la compañía debe ser de uso exclusivo para asuntos relacionados con la empresa. Cualquier excepción a esta política debe ser autorizada por la Gerencia General, Dirección Comercial y Operativa, Dirección Administrativa y Financiera o jefe de Tecnología.

- ✓ Abstenerse de usar sitios que salten la seguridad del servidor de acceso a internet (proxy), la única excepción a esta política será las revisiones de Auditoría Externa en Seguridad Informática.

- ✓ El uso con fines comerciales, políticos, particulares u otro que no sea laboral y que dio origen a la habilitación del servicio, no está permitido.

- ✓ Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma algos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.

- ✓ Los colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona.

- ✓ Abstenerse de coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley local, nacional o internacional; incluyendo, pero no limitado, las leyes y regulaciones de control y exportación de Colombia y de los decretos sobre fraudes de computación.

- ✓ Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social, marital, ocupacional, financiera y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la Compañía y violatorias a la ley 1581 del 2012.

- ✓ Los colaboradores se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.

- ✓ Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como “cartas en cadena” o “las pirámides”, son faltas se constituyen como violaciones a esta política.

- ✓ No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.

- ✓ Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios" ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta política.

5.5 Uso de herramientas que comprometen la seguridad

Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la Jefatura de Tecnología, cualquiera de los siguientes actos.

- ✓ Acceder al sistema o red
- ✓ Monitorear datos o tráfico.
- ✓ Sondear, copiar, probar firewalls o herramientas de hacking.
- ✓ Atentar contra la vulnerabilidad del sistema o redes.
- ✓ Violar las medidas de seguridad o las rutinas de autenticación del sistema o red.

5.6 Recursos compartidos

El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso y aplicación debe ser controlado.

Con este propósito la organización define los siguientes lineamientos para su uso seguro:

- ✓ El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

- ✓ El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesiten y deben ser protegidas con contraseñas.

- ✓ No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

- ✓ Sitios web para compartir documentos.

- ✓ El dueño del sitio será el responsable de la seguridad del mismo y del acceso a la información que se encuentra alojada.

- ✓ El dueño del sitio será el responsable de otorgar los permisos requeridos.

- ✓ El dueño del sitio definirá un delegado que tenga control total sobre el sitio, a manera de

contingencia, para la asignación de los permisos requeridos en su ausencia.

- ✓ Ninguna información de COMBUSTIBLES DE COLOMBIA S.A. podrá utilizar tecnologías de computación En la nube si no está previamente autorizado por la Jefatura de Tecnología.

5.7 Uso equipos portátiles y dispositivos móviles

Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorio y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- ✓ El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.
- ✓ El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón, huella dactilar reconocimiento de voz, entre otras.
- ✓ Uso de aplicación de antivirus.
- ✓ Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.
- ✓ En caso de pérdida del equipo celular, se debería notificar al área de tecnología para realizar el borrado remoto de los datos de la cuenta corporativa.

5.8 Acceso de equipos distintos a los asignados

- ✓ Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.
- ✓ No dejar claves en ningún sistema de almacenamiento de información web.
- ✓ Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
- ✓ Cerrado de sesión de escritorio virtual cuando no esté en uso.

La Jefatura de Tecnología debe implementar medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se comprometa la información del negocio. Teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.

La utilización de los servicios móviles conectados a las redes, debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación

móvil, solo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control de acceso.

La Jefatura de Tecnología, conforme la clasificación de activos de información, debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, perdida, fuga, consulta, uso o acceso no autorizado o fraudulento.
El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgara acceso a menos que sea explícitamente permitido.

5.9 Registro de usuarios

Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizara para el seguimiento de las actividades de responsable individual o jurídica. Las actividades habituales de usuario no deben ser desempeñadas a través de cuentas privilegiadas.

En circunstancias excepcionales, por beneficio de la compaña, se podrá usar un identificador compartido, para un grupo de usuarios con trabajo específico; este debe ser autorizado y debidamente aprobado por la respectiva área de Tecnología.

El usuario debe tener autorización de la respectiva área de Gerencia, Dirección Comercial y Operativa, Dirección Administrativa y Financiera para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la empresa y conserven una adecuada segregación de funciones. Adicionalmente, debe tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

5.10 Responsabilidades del usuario

Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, el jefe de Área de Tecnología implementara los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario implementar un procedimiento de revisión periódica de los permisos de acceso de los usuarios.

Los colaboradores, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este. Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

5.11 Control de acceso a la red

Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

5.12 Control de acceso a las aplicaciones

El uso de programas que pueden ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.

Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o software.

5.13 Política de usuarios y contraseñas

La asignación de usuarios y contraseñas es un permiso que Combuscol SA concede a sus funcionarios, con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información.
La política de seguridad de usuarios y contraseñas tiene como objetivo principal establecer reglas y directrices para garantizar un uso seguro y protegido de los sistemas de información de Combuscol SA

Anexo; Política usuarios y contraseñas

5.14 Política de Escritorio limpio.

Establecer la política de Escritorio y Pantalla Limpia para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

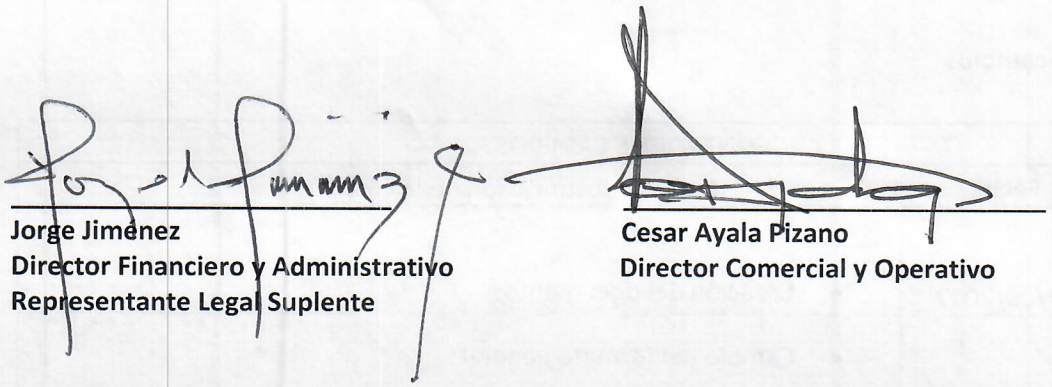
Anexo; Política de escritorio limpio

5.15 Control de cambios

CONTROL DE CAMBIOS		
Versión	Fecha	Justificación de la versión
1	07/06/2017	• Creación del documento.
2	22/10/2019	• Cambio del formato general. • Actualización de la política de seguridad de la información
3	22/10/2018	• Actualización a formato estándar • Eliminar nombres de funcionarios y reemplazarlos con cargos • Actualización normatividad ley 1581 de 2012 • Complementar con los contratos de transmisión de datos personales (Área de Auditoria Interna)
4	27/06/2023	• Se anexa política de usuarios y contraseñas y se actualizan firmas.
5	11/8/2023	• Separar políticas de seguridad de la información de los procedimientos. • Se anexa Políticas de escritorio limpio, y usuarios y contraseñas • Restricciones uso de correo • Solicitud eliminación de dispositivos móviles.

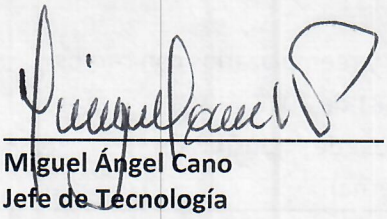
APROBACION

Se firma en señal de aprobación las Políticas de Seguridad de la Información de Combuscol S.A.



Jorge Jiménez
Director Financiero y Administrativo
Representante Legal Suplente

Cesar Ayala Pizano
Director Comercial y Operativo



Miguel Ángel Cano
Jefe de Tecnología