POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Revisó: Comité de Seguridad de la Información.

Aprobó: Gerencia General

TABLA DE CONTENIDO

INTRODUCCIÓN 3
POLÍTICAS GENERALES Y BUENAS PRÁCTICAS POR PARTE DELOS COLABORADORES 4
POLÍTICA DE ACCESO A INTERNET 8
SIS-PO-01 8
POLITICA DE CONTROL AL SOFTWARE 11
SIS-PO-02 11
ACCESO A LAS ESTACIONES DE TRABAJO 13
SIS-PO-03 13
CONFIDENCIALIDAD DE LAS CONTRASEÑAS 14
SIS-PO-04 14
POLITICAS DE INGENIERIA SOCIAL 16
SIS-PO-05 16
POLÍTICAS DE CATALOGACIÓN DE LA INFORMACIÓN 20
SIS-PO-06 20
POLÍTICAS PARA EL CONTROL DE HARDWARE 24
SIS-PO-07 24
POLÍTICA DE USO DE CORREO ELECTRÓNICO 27
SIS-PO-08 27
CONSECUENCIAS POR EL MAL USO DE LOS SERVICIOS 32

INTRODUCCIÓN

Las empresas modernas, cada vez más dependientes de la tecnología, por ende de la Jefatura de Tecnología y Sistemas de Información, enfrentan una serie de riesgos por cuenta de las herramientas que apoyan su negocio. Virus, spyware, Hardware, keyloggers, phishing y spam, entre otros, son un riesgo constante y silencioso que acecha en cada computador conectado a Internet. Sin embargo, en algunas ocasiones los principales daños son causados de forma voluntaria o accidental, por los propios colaboradores.

Incluso es posible que los colaboradores se vean involucrados sin intención, en delitos de robo, de datos críticos de la compañía o la suplantación de identidad.

Un portátil con información de la empresa que le sea robado a un colaborador en cualquier lugar o circunstancia (cuyos datos no están codificados), una memoria USB con información confidencial que se deja olvidada en algún lugar o un correo electrónico que contenga en los archivos virus que se propaga por la red, son algunos ejemplos de acciones involuntarias que generan un gran daño y perjuicio a la compañía.

Todo esto, se evita con unas políticas claras y de conocimiento de toda la Compañía sobre Seguridad de la Información. Para lo cual COOTRADIAN, ha elaborado, el presente documento, en el cual se especifican las políticas y buenas prácticas a tener en cuenta por parte de los colaboradores respecto de la Seguridad de la Información.

POLÍTICAS GENERALES Y BUENAS PRÁCTICAS POR PARTE DE LOS COLABORADORES.

1. COOTRADIAN cuenta con las licencias de todos los programas de software que utiliza. La empresa no es propietaria de ese software o de sus manuales y, por tanto no tiene derecho a reproducirlo, salvo autorización del titular de los derechos de autor.

2. Cualquier copia de un programa de computador, excepto aquellas realizadas con fines de seguridad o archivo, es una violación a la legislación sobre derechos de autor. Cada programa que la empresa adquiera legalmente, es para uso exclusivo en cada uno de los computadores. Si el computador tiene una copia de un software instalada en el disco duro, ese programa no debe ser copiado en ningún otro disco duro.

3. Los colaboradores de la empresa, que tengan conocimiento de cualquier uso indebido del software por parte de cualquier colaborador, deberán notificar este hecho al jefe de su departamento o al Responsable de Seguridad de la Información (Jefatura de Tecnología y Sistemas de Información) para que se tomen las acciones del caso.

4. Los colaboradores de COOTRADIAN deben respetar y acatar los derechos de Propiedad Intelectual, de conformidad con las disposiciones legales vigentes y con los convenios internacionales que le sean aplicables, de acuerdo con las Leyes: Ley 23 de 1982, Ley 44 de 1993 y Ley 603 de 2000 y la normatividad vigente al respecto.

5. COOTRADIAN no permite, ni autoriza ningún tipo de copia ilegal de programas. Los colaboradores que violen o incurran en dichas disposiciones o en los acuerdos de licencias de software, la Gerencia de Gestión Humana o quien haga sus veces, procederá a iniciar un proceso disciplinario y a la aplicación de las medidas administrativas que se deriven de este, incluso será justa causa de terminación de contrato.

6. AUDITORIA.- En cualquier momento el área encargada efectuará auditorías a los diferentes computadores de la Compañía, con el fin de verificar que no se encuentren software no autorizados o ni legalizados.

7. La tecnología informática – hardware, software, redes y la información que contienen – son propiedad exclusiva de COOTRADIAN, y son de fundamental importancia para el éxito del negocio. Todo colaborador que utilice un computador de propiedad de COOTRADIAN, tiene la responsabilidad de utilizar esta herramienta correctamente y para los fines comerciales para los que fueron creados y para los cuales se le otorgó el permiso.

Esto significa que:

- Las computadoras de la compañía deben utilizarse de manera responsable y principalmente para fines comerciales o laborales legítimos.

- La seguridad de los sistemas de computación, incluyendo los datos corporativos, comunicaciones electrónicas y aplicaciones (software), deben estar protegidos todo el tiempo.

- Las comunicaciones electrónicas que pueden considerarse ofensivas, derogatorias, difamatorias, hostiles, obscenas o vulgares están prohibidas.

- Está prohibido utilizar los sistemas de comunicación electrónicos de la Compañía para divulgar incorrectamente materiales con derechos de propiedad intelectual o protegidos bajo licencia.

- Todo colaborador, debe proteger y salvaguardar la información utilizada y entregada por la empresa para acceder a las redes de la Compañía, incluidos los nombres de usuario y contraseña.

- Cada colaborador autorizará a las Directivas de COOTRADIAN o quienes ella delegue para acceder y revisar los equipos que tiene asignado para desarrollar sus tareas, la información que este contenga, todas las comunicaciones, registros e información creados en el trabajo o con los recursos de la compañía.

    - Si algún colaborador necesita saber si determinada información puede ser enviada por el correo electrónico corporativo, se debe comunicar con su jefe inmediato. En caso de necesitar información acerca de la seguridad de las computadoras y las redes, se deberá comunicar con la Jefatura de Tecnología y Sistemas de Información.

8. Información Confidencial, Propiedad Intelectual e Información Propiedad de Terceros

Nuestra Compañía continuamente desarrolla ideas, estrategias y otro tipo de información comercial valiosa, la cual no es del dominio público. En tal sentido, COOTRADIAN es dueña de esta información confidencial, así como también de otros tipos de bienes, tales como: bases de datos de ventas, de marketing y otros tipos de bases de datos de la compañía; estrategias y planes de marketing; información de precios; registros de clientes y colaboradores; propuestas y desarrollo de productos nuevos, etc. Debido a que esta información es el resultado del trabajo arduo de nuestra compañía, varias leyes permiten que COOTRADIAN proteja dicha información del uso que personas ajenas puedan hacer de la información.

Esto significa que:

- Todos los colaboradores deben proteger la confidencialidad de la información de propiedad de COOTRADIAN para garantizar que recibamos los beneficios de nuestro trabajo.

- Todos los colaboradores deben respetar, cumplir y acatar el otrosí sobre el acuerdo de confidencialidad que se suscribe por los nuevos colaboradores al ingresar a laborar en COOTRADIAN, o el que fue firmado por todos los colaboradores activos a la fecha.

- Los colaboradores de COOTRADIAN, se abstendrán de comunicar en lugares públicos dicha información confidencial, evitando con esto que la misma se pueda filtrar y tener conocimiento público.

- Ningún colaborador podrá transmitir, ni divulgar información de carácter confidencial y de propiedad única y exclusiva de COOTRADIAN , a través de Internet, redes sociales, correo electrónico corporativo hacia correos electrónicos personales o de terceras personas, ni siquiera entre colaboradores de la entidad, salvo, autorización expresa del Empleador.

- En caso de ser necesario divulgar algún tipo de información confidencial entre personas ajenas a la compañía, se deberá solicitar una autorización previa por escrito al gerente y firmar un acuerdo de confidencialidad por escrito, aprobado por el Responsable de Seguridad de la Información o asesor legal.

9. Bienes y Tiempo de la Compañía

Los bienes de la compañía se utilizarán únicamente para las operaciones comerciales de la misma. El uso que debe hacer cada colaborador de los bienes asignados para su labor, deben ser cuidados y protegidos mientras se encuentren en poder del este, evitando con esto la malversación o el robo de los mismos.

Esto significa que:

- Los colaboradores deben ser responsables de las herramientas asignadas en su trabajo y el buen uso que hagan de estos.

- Los activos de la compañía deberán protegerse de la malversación, desviación o el robo. Toda sospecha de adulteración, robo o falta de control interno de los productos u otros activos deberá reportarse al Responsable de Seguridad de la Información (Unidad de Tecnología).

- Durante las horas de trabajo, cada colaborador deberá velar por que no interfieran los intereses externos tales como: Actividades de entretenimiento en internet, videos, música, juegos, etc. con sus responsabilidades laborales.

POLÍTICA DE ACCESO A INTERNET

SGSI-PO-01	
OBJETIVO	Establecer y difundir las políticas relacionadas con el manejo y control de utilización de Internet, de tal forma que se garantice el normal y efectivo uso de ésta herramienta.
ALCANCE	A nivel Nacional para todos los colaboradores de COOTRADIAN , tanto en la oficina principal como en Sucursales y todo usuario de la red de COOTRADIAN

DESARROLLO DE LA POLITICA

1.1 **Políticas Generales**

1.1.1 Los colaboradores son responsables por usar los sistemas de comunicación de COOTRADIAN, de una manera adecuada, ética y legal y en concordancia con la presente política.

1.1.2 Todos los equipos de cómputo conectados a la red de la compañía y que se encuentre dentro del Dominio refisal.com.co y/o Refisal1 tienen acceso a Internet.

1.2 **Políticas Especificas**

1.2.1 Políticas de Uso de Acceso a Internet:

1.2.1.1 Está permitido el acceso a páginas de información financiera, técnica, comercial, cultural, etc. a las cuales por desarrollo de las actividades propias de cada puesto de trabajo sea necesario ingresar para consultar información que mejore nuestras labores diarias.

1.2.1.2 El uso del acceso a Internet debe ser única y exclusivamente para propósitos laborales y comerciales.

1.2.1.3 El uso de la herramienta para fines personales, debe realizarse en horario "No Laboral" o en la hora de almuerzo, para no interferir con el buen funcionamiento de los servicios web prestados por COOTRADIAN propios del desarrollo exitoso del negocio y con el desempeño de las labores asignadas a cada empleado.

1.2.2 Los colaboradores de COOTRADIAN no podrán utilizar el acceso a Internet para los siguientes propósitos:

- Utilizar los recursos de la red de COOTRADIAN para acceder sin las autorizaciones correspondientes a redes y sistemas remotos.
- Utilizar los servicios de red para juegos a través del servicio de Internet.
- Utilizar los servicios de red para contenido multimedia en línea catalogado como "streaming de audio o video". P. ej: Youtube, radio, etc.
- Utilizar los servicios de red para ver cualquier tipo de material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las políticas internas de COOTRADIAN
- Utilizar los servicios de Internet para enviar archivos o publicar datos que sean confidenciales y de propiedad exclusiva de COOTRADIAN. La Jefatura de Tecnología y Sistemas de Información o el responsable de Seguridad de la Información reportara a la Gerencia, los archivos que salgan de la compañía por medio de los accesos de Internet, y en caso de ser necesario, se deberá reportar el caso a Gestión Humana, para dar inicio al proceso disciplinario y aplicar las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.
- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular o de beneficio propio, ajenas a la razón social de COOTRADIAN.
- Utilizar los servicios de Internet para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), marcas registradas, secretos comerciales u otros de propiedad intelectual.

- Está prohibido que cualquier colaborador se valga de los medios electrónicos, las herramientas de trabajo, el acceso a las redes sociales al interior de las instalaciones de COOTRADIAN para perjudicar, o vulnerar los derechos de los menores de edad, o incurrir en cualquier delito que ponga en vilo la integridad de los menores de edad.

- El acceso no autorizado o cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidad de un sistema o red, violando las medidas de seguridad o de autenticación sin la expresa autorización del propietario del sistema o de la red.

- La interferencia con el servicio de cualquier usuario, huésped (host) o red, incluyendo el envío de correo no solicitado en grandes cantidades, destinado a paralizar un servidor (mailbombing), inundaciones (flooding), intentos de sobrecargar (overload) el sistema y de ataques anunciados (broadcast attacks).

- Hacerse pasar por algún colaborador o Directivo de COOTRADIAN o fingir ser cualquier otra persona o entidad que sea cliente, potencial cliente o proveedor de COOTRADIAN, incluyendo, sin limitación, o cualquier otro modo de mentirle a COOTRADIAN como empleador, o fingir sobre su relación personal o sentimental con cualquier otra persona o afiliación a cualquier entidad salud, pensiones, entidades educativas, financieras entre otras.

- Falsificar rúbricas o de otro modo manipular identificativos con el fin de disfrazar la naturaleza del contenido transmitido a través del Servicio.

- "Acechar" o de algún modo hostigar a terceros, o recoger o almacenar información personal sobre otros usuarios.

- No se podrán utilizar los servicios de Internet corporativo para establecer sesiones de conexión remota tales como teamviewer, vnc, etc., solo se aceptan estas sesiones a personal de la Jefatura de Tecnología y Sistemas de Informacióny con fines de soporte remoto.

1.2.3 Las contraseñas de acceso a Internet (que son las mismas de la red) deben ser estrictamente confidenciales y personales para asegurar un alto nivel de seguridad en la red de comunicaciones de COOTRADIAN, y deben ser usadas a la luz de las políticas establecidas por la compañía para ello.

1.2.4 Los servicios de Internet deben ser monitoreados, por lo tanto, cualquier material descargado o de cualquier modo obtenido a través del uso del servicio, se realiza a su exclusiva discreción y riesgo y el funcionario será el único responsable por cualquier daño producido a su sistema informático o por cualquier pérdida de datos derivada de descargar dicho material.

POLITICA DE CONTROL AL SOFTWARE

SGSI-PO-02	
OBJETIVO	La política de control al software tiene como objetivo el establecer las normas que rigen la utilización del software instalado por COOTRADIAN, así como las normas que rigen el software no autorizado instalado. Las normas establecidas en esta política cubren los esquemas de licenciamiento actual de COOTRADIAN, pero no están limitadas, por lo cual se podrán tomar decisiones adicionales o complementarias a dichas normas.
ALCANCE	Aplica para todas la personas que estén conectadas a la red de COOTRADIAN Rige para todo tipo de software, a continuación se describen algunos ejemplos: • Sistemas Operativos:, Ej: Windows XP, Windows 2000, Windows Vista, Windows 7, etc. • Utilitarios de Oficina:, Ej: Word, Excel, Power Point, Project, etc. • Herramientas de Graficación: Ej: Visio, Corel Draw, etc. • Administradores de Bases de Datos:, Ej: Access, SQL, DB2, etc. • Otros: Ej: Enciclopedias, juegos, Software para ejecución de archivos MP3, etc.

DESARROLLO DE LA POLITICA

1. Políticas Generales

1.1. El Software solo podrá ser instalado por el personal de Tecnología de COOTRADIAN , previa autorización del Jefe y/o el coordinador de la Jefatura de Tecnología y Sistemas de Información, el software no incluido dentro del estándar, deberá ser solicitado únicamente por los Gerentes o Directores con aprobación de la Gerencia, la Jefatura de Tecnología y Sistemas de Información hará un estudio técnico del producto así como un análisis Costo/Beneficio del mismo y definirá si se autoriza o no la compra del software.

1.2. Toda adquisición de Software nuevo que sea necesario para el soporte de actividades de las diferentes áreas será adquirido a través de la Jefatura de Tecnología y Sistemas de Información, quien finalmente administrará la licencia y los medios. Ningún colaborador de la compañía está autorizado para adquirir software sin la aprobación de la Jefatura de Tecnología y Sistemas de Información.

1.3. La Jefatura de Tecnología y Sistemas de Información implementará los controles necesarios y reportará mensualmente al comité de Seguridad de la Información, los usuarios que tienen instalado software no autorizado, con el fin de tomar las acciones necesarias para garantizar el cumplimiento de esta política.

1.4. La Jefatura de Tecnología y Sistemas de Información podrá mediante la utilización del software de control de Inventarios de Hardware y Software hacer auditorias permanentes a los computadores y podrá desinstalar cualquier software no autorizado y no reportado sin previo aviso, archivos de usuario que se consideren como material irrespetuoso o pornográfico, así como también archivos de música, mp3, almacenamiento de fotografías personales del funcionario, y cualquier otro no autorizado por la Compañía. Adicionalmente se reportará a la Gerencia y a Gestión Humana, sobre el resultado de dichas revisiones.

1.5. Toda persona conectada a la red de COOTRADIAN que detecte algún tipo de software ilegal debe informar de inmediato al Responsable de Seguridad de la Información para realizar el procedimiento respectivo de desinstalación de este.

ACCESO A LAS ESTACIONES DE TRABAJO

SGSI-PO-03	
OBJETIVO	Velar por la confidencialidad de la información almacenada en las estaciones de trabajo cuya responsabilidad está en cabeza de algún usuario específico.
ALCANCE	Aplica para todas la personas que estén conectadas a la red de COOTRADIAN

DESARROLLO DE LA POLITICA

1. Políticas Generales

El personal que no es titular de un computador ó estación de trabajo no puede acceder en cualquier computador de la Compañía a menos que:

1. Obtenga autorización expresa del usuario responsable o jefe del usuario responsable o del encargado de la sección o área de la cual se quiere usar el computador.

2. Cuente con un usuario y clave para acceder a la red a través de esa estación de trabajo o computador.

3. Se haga responsable por la información existente en su perfil y en las carpetas compartidas a las cuales tiene privilegios de modificación, en el computador que piensa usar.

Si algún usuario de la Compañía omite las anteriores recomendaciones y usa un computador que no está bajo su responsabilidad, asume el riesgo de ser sancionado por pérdida de archivos previa demostración por parte de los sistemas de seguridad, logs del sistema que comprueben esto, a demás de dar inicio al proceso disciplinario respectivo.

Los usuarios definidos como responsables de un activo informático de tipo estación de trabajo o computador, deben asegurar que no se conecten módems inalámbricos en el computador bajo su responsabilidad, con el fin de acceder a internet desde este punto. Es importante recordar que este tipo de conexiones va en contra de las políticas tecnológicas definidas en los firewalls de

COOTRADIAN El uso de estos dispositivos, será exclusivo para personal autorizado por la Jefatura de Tecnología y Sistemas de Información de COOTRADIAN

En caso de incurrir en este tipo de situaciones o violaciones a la política de acceso a las estaciones de trabajo, se deberá informar a la Gerencia de Gestión Humana, con el fin de dar inicio al proceso disciplinario respectivo y así a la aplicación de las medidas administrativas correspondientes.

CONFIDENCIALIDAD DE LAS CONTRASEÑAS

SGSI-PO-04	
OBJETIVO	Velar por la confidencialidad de las contraseñas de acceso a los diferentes sistemas de la Compañía.
ALCANCE	Aplica para todas la personas que estén conectadas a la red de COOTRADIAN

DESARROLLO DE LA POLITICA

2. Políticas Generales

Los usuarios deben establecer contraseñas acorde con las recomendaciones dadas por la Jefatura de Tecnología y Sistemas de Información, las cuales son:

- Mantener las contraseñas en secreto;
- Evitar mantener un registro en papel de las contraseñas, a menos que esta pueda ser almacenada en forma segura;

- Cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

- Seleccionar contraseñas de calidad, con una longitud mínima de ocho caracteres que:

    - Sean fáciles de recordar;

    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ej. Nombres, números de teléfono, fecha de nacimiento, etc.;

    - No tenga caracteres idénticos, consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

    - Cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios, deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas;

    - Cambiar las contraseñas provisorias en el primer inicio de sesión.

    - No incluir contraseñas en los procesos automatizados de inicio de sesión, por ej. Aquellas almacenadas en una tecla de función o macro;

    - No compartir las contraseñas individuales de usuario;

    - Nunca se debe compartir la contraseña, en caso de ser necesario, se debe notificar vía correo electrónico al jefe inmediato por escrito, con copia al Responsable de Seguridad de la información (Jefatura de Tecnología y Sistemas de Información), con la debida justificación.

Es importante recordar que la información que cada usuario maneja, es de su absoluta responsabilidad, al igual que las situaciones que presenten bajo el usuario de red asignado, como son:

1. Ejecución de programas no autorizados y no avalados por la Jefatura de Tecnología y Sistemas de Información.

2. Violación a la POLÍTICA DE ACCESO A INTERNET.

3. Propagación de un virus desde el computador al cual el usuario esta registrado como usuario vigente.

En caso de presentarse alguna de estas situaciones irregulares y prohibidas, cada usuario será el responsable directo, por lo cual, en caso de incurrir en este tipo de situaciones o violaciones a la política de acceso a las confidencialidad de las contraseñas, se deberá informar a la Gerencia de Gestión Humana, con el fin de dar inicio al proceso disciplinario respectivo y así a la aplicación de las medidas administrativas correspondientes.

POLITICAS DE INGENIERIA SOCIAL

SGSI-PO-05	
OBJETIVO	Establecer y dar a conocer las pautas y parámetros a seguir por parte de colaboradores y externos vinculados con la operación de COOTRADIAN y sus filiales, el manejo de la información que se suministre de manera verbal, por escrito o por cualquier otro medio. A demás de prevenir que los colaboradores, personal externo o terceros no autorizados, puedan acceder u obtener información sensible de la compañía o incluso los dos últimos a ingresar a las instalaciones, sucursales o a lugares restringidos, mediante el uso de engaños o artimañas, con el propósito de cometer algún ilícito o para obtener para sí o para otros, algún beneficio.
ALCANCE	A nivel Nacional para todos los colaboradores o externos vinculados con la operación de COOTRADIAN y sus filiales.

DESARROLLO DE LA POLITICA

1. DEFINICIONES:

a. **Ingeniería Social:** Se denomina así a todas aquellas conductas utilizadas por algunas personas valiéndose de la psicología, tretas o engaños, para sacar información sensible o acceder a ciertos lugares, sin que la otra u otras personas se den cuenta del engaño al que están siendo víctimas. En términos generales, la Ingeniería Social, consiste en la manipulación de las personas, para que voluntariamente realicen actos que normalmente no harían, convirtiéndose en el método de ataque más sencillo a la seguridad de una compañía, el menos peligroso y el más efectivo.

b. **Usuario:** Persona conectada a la red de las compañías o a sus sistemas centrales la cual utiliza estas herramientas, para la realización de sus labores diarias.

c. **Atacante:** Quien se aprovecha de la buena fe de las personas, en este caso, de los usuarios, para lograr sus propósitos.

d. **Psicología de Ataque:** Principal herramienta utilizada por las personas que desean obtener información o acceder a sitios o lugares que de otra forma no se permitirían. El atacante se aprovecha de sentimientos variados de las personas como la curiosidad, la avaricia, el sexo, la compasión, el miedo, entre otros, para engañar o persuadir a otros, sin que éstos se den cuenta que los están manipulado para lograr sus objetivos.

2. POLITICAS :

2.1 Políticas Generales:

2.1.1 Todos los colaboradores deberán tener un especial cuidado de cara a los clientes internos, externos o terceros no autorizados, el cuidado en la seguridad de la información y estar atentos a cualquier intento por parte de estos la obtención de información que compete solo a quien es responsable por su manejo y administración.

2.1.2 Ningún colaborador deberá asumir como válido un comportamiento de un tercero o de un colaborador no autorizado, pretender recibir favores o prebendas especiales por fuera del cumplimiento de las políticas y procedimientos de la Compañía. Es importante que el responsable de custodiar la información o el funcionario del área encargada, valide y confirmen la información solicitada por este tercero no autorizado o a lugares a los que pretende acceder y que son restringidos tanto para el funcionario como para el tercero no autorizado.

2.1.3 Para los casos en los que un tercero o colaborador no autorizado, argumenta ser conocido, amigo o tener relaciones muy cercanas con el Gerente General de la compañía, o con algún gerente u otro colaborador de alto nivel, con el fin de que le permitan obtener información o acceder a las instalaciones de la compañía o a algún sitio restringido o retirar algún elemento de las instalaciones de la compañía, se debe validar directamente con la Gerencia General o con la Jefatura de Tecnología y Sistemas de Información.

2.1.4 Todo colaborador, deberá estar atento cuando ingrese a las instalaciones de la Compañía, evidenciando a aquellas personas que se aprovechan de la marcación de la tarjeta o la apertura de una puerta, para ingresar a las instalaciones de la compañía. Sin excepción, Toda persona, que no sea colaborador de la Compañía, deberá anunciarse en la recepción y seguir los procedimientos establecidos de control y acceso de personas al edificio o a las oficinas de la Compañía. Todos los colaboradores, deberán informar cualquier situación sospechosa a su superior, al Responsable de Seguridad de la Información o a la Gerencia respectiva.

2.1.5 No se deberá suministrar ni informar telefónicamente, datos confidenciales de los colaboradores, así como no transferir llamadas, sin el debido consentimiento o autorización de la persona a la que se solicita.

2.1.6 Cualquier colaborador deberá verificar previamente la veracidad de la fuente que solicita cualquier información sobre la localización en tiempo y lugar del Gerente General o de alguno de los Directivos de la Compañía.

2.1.7 Todos los colaboradores deberán estar atentos, cuando un tercero utilizando la psicología de ataque, intente persuadirlo con el fin de que incumpla con las políticas de la compañía o entregue información sensible o elementos de un área, bajo el argumento que fue enviado por alguien o que ya tiene la debida autorización. Siempre se deberá indagar, comprobar, y verificar antes de entregar cualquier documento, objeto, bien mueble o permitir el acceso a lugares restringidos o a las instalaciones de la compañía. Se deberá validar con la fuente o el contacto según el caso.

2.1.8 No se deberá entregar información relevante de la compañía, de sus Directivos o colaboradores, a personas que lo soliciten vía telefónica, ya que con esto se estaría poniendo en riesgo la seguridad y la vida de alguno de ellos Si se tienen sospechas o se trata de alguna situación sospechosa e irregular, deberá ser reportada a la Gerencia General o al Responsable de Seguridad de la Información.

2.1.9 Todos los colaboradores deberán abstenerse de generar situaciones de riesgo comunicando a terceros no autorizados o a colaboradores de otras áreas, posibles debilidades de control al interior de los procesos o del sistema, ya que puede ser usado por otros, en beneficio propio. El atacante utiliza sus artimañas sin conocimiento del funcionario. .

2.1.10 Toda información recibida por vía e-mail en la que se presenten títulos invitando a abrir un archivo o a replicar hacia otros o a descargar o diligenciar información sensible por parte del funcionario, deberá ser reportada al superior o al Responsable de Seguridad de la Información para su análisis. El colaborador deberá abstenerse de abrir o retransmitir el archivo, toda vez que puede ser un engaño para invadir la red con un virus o para obtener las claves de acceso y vulnerar la seguridad de los sistemas de la compañía.

2.1.11 No se deberán ejecutar programas de procedencia desconocida, si el remitente es alguien desconocido o el título del mensaje no es claro o es sospechoso, el colaborador se deberá abstener de abrirlo y deberá reportar de inmediato la situación a su superior o al Responsable de Seguridad de la Información.

2.1.12 No se deberá informar telefónicamente las características técnicas de la Red, sus localizaciones o personas a cargo de la misma. Se debe reportar de inmediato el hecho a la Jefatura de Tecnología y Sistemas de Informacióno al Responsable de Seguridad de la Información.

2.1.13 Ninguna persona diferente a las autorizadas por la Jefatura de Tecnología y Sistemas de Informaciónpuede instalar parches o ejecutar programas de fuentes desconocidas, ya que se puede tratar de un posible virus que pone en riesgo la seguridad de la red de COOTRADIAN

2.1.14 Ningún colaborador debe diligenciar electrónicamente o en formatos impresos, encuestas que ofrezcan premios o beneficios especiales en las que se deban registrar sus password o claves. Se debe indagar con el Responsable de Seguridad de la Información o comente a su superior el hecho, para que se tomen las medidas pertinentes o se evalúe la situación.

2.1.15 No se debe divulgar a los compañeros de trabajo o a personal externo, la información que se administre y que ha sido clasificada como confidencial o restringida, a la luz de las políticas de Catalogación de Información de COOTRADIAN

2.1.16 Si algún colaborador observa comportamientos en sus compañeros de trabajo que puedan estar poniendo en riesgo la información de COOTRADIAN, sus activos o la vida o seguridad de otros colaboradores o directivos de la compañía, deberá reportarlo de inmediato a su superior, al Responsable de Seguridad de la Información o a la Gerencia.

3. SANCIONES

El incumplimiento a cualquiera de las anteriores políticas puede poner en riesgo la información, los elementos o las personas de COOTRADIAN, es por ello que todo colaborador deberá velar porque se cumplan y de detectarse incumplimientos, deberán ser reportados al Responsable de Seguridad de la Información quién después de realizar un análisis, determinará si lo reporta a la Gerencia de Gestión Humana o Gerencia General, para su evaluación y toma de medidas pertinentes.

POLÍTICAS DE CATALOGACIÓN DE LA INFORMACIÓN

SIS-PO-06	
OBJETIVO	Establecer y dar a conocer las pautas y parámetros a seguir para el manejo de la información que se encuentra en medio físico, magnético (DVD, CD, archivo, Attachment en e-mail) y en carpetas compartidas en el equipo de computo, con el fin de mantener una metodología que permita ejercer un control sobre ésta, identificando claramente responsables y dueños de la información de COOTRADIAN
ALCANCE	A nivel Nacional, sobre toda la información de COOTRADIAN Esta política adicionalmente, contempla aquella información perteneciente a terceros u otras entidades, la cual ha sido confiada a COOTRADIAN bajo acuerdos de confidencialidad o contratos.

DESARROLLO DE LA POLITICA

1. DEFINICIONES:

1.1 Información No Clasificada: Declarada como pública, puede ser libremente entregada a personas no autorizadas sin causar daño a la compañía.

1.2 Información de Uso Interno: Declarada como de uso exclusivo para los colaboradores de COOTRADIAN y de sus socios de negocio, no podrá ser entregada a terceros.

1.3 Información Confidencial: Es aquella más sensible y que en manos de terceros, puede poner en riesgo el negocio.

1.4 Información Restringida: Declarada como secreta y de uso exclusivo de las personas que COOTRADIAN determine como autorizadas.

1.5 Confidencialidad: La información de los sistemas, es accedida solo por usuarios autorizados.

1.6 Integridad: La información de los sistemas, sólo puede ser creada y modificada por los usuarios autorizados.

1.7 Disponibilidad: La información siempre está disponible cuando se necesita.

1.8 Acceso a la Información: Se refiere a tener la autorización para poder consultar, modificar, borrar o reproducir información.

1.9 Uso de la Información: Se refiere a lo que se hace con la información, es pertinente a las responsabilidades y funciones de quien la está trabajando.

1.10 Administración de la Información: Se refiere a características tales como cuidado, respaldo, no alteración, acceso, distribución de la información.

1.11 Distribución de la Información: Se refiere a los medios, a las personas y a la información misma que puede ser distribuida o enviada a terceros por los que se puede enviar la información.

1.12 Retención de la Información: Se refiere al tiempo durante el cual debe conservarse la información, antes de ser desechada o pasada a otro medio.

1.13 Destrucción de la información Se refiere a los procedimientos que deben ser aplicados para deshacerse de la información tanto física como magnética, para evitar su posterior lectura o recuperación.

2. Políticas Generales:

2.1.1 Las Gerencias dueñas de la información, deben asociar cada tipo de información pertinentes a sus áreas, en tres niveles de catalogación establecidos así:

- De uso general (Pública).
- Restringida.
- Confidencial.

2.1.2 En las políticas de Uso y Manejo de la Información Catalogada, deben estar contempladas las políticas que permiten avalar aspectos tales como: Acceso, uso, administración, distribución, retención y destrucción de la información de COOTRADIAN Dichas políticas deben ser diseñadas por las Gerencias o Unidades dueñas de la Información.

2.2 Políticas Específicas:

4.2.1 La Información Confidencial debe ser protegida en medios seguros, definiendo seguro como el medio que cuenta con las características para evitar que la información se pierda, sea alterada o accedida por personas no autorizadas por COOTRADIAN Para todos los colaboradores de COOTRADIAN , los únicos tres medios donde se deberá almacenar información relacionada con las funciones propias de cada puesto de trabajo son:

a) Localmente en cada computador en la unidad C:, en la subcarpeta Datos_COOTRADIAN. Es decir carpeta local de cada computador (\Mis Documentos\Datos_COOTRADIAN). ***Aplica solo si se activa la CDP para respaldar estaciones de trabajo.***

b) \Datos_COOTRADIAN), de computadores involucrados en procesos críticos será respaldada periódicamente por la Jefatura de Tecnología y Sistemas de Información.

c) En las carpetas compartidas de Red.- Información o archivos que se deben compartir con dos o más usuarios y que es de bajo nivel de consulta. Se debe aplicar los principios de necesidad de saber y de menor privilegio posible, es decir, crear tantas carpetas como sean necesarias para ser accedidas por los usuarios que les corresponde saber de esta información y establecer el privilegio adecuado (consulta o modificación). Esta información será respaldada automáticamente todos los días y en línea por la Jefatura de Tecnología y Sistemas de Información.

d) En la Intranet de COOTRADIAN.- Información o archivos que se deben compartir con dos o más usuarios y que es de alto nivel de consulta. En cada unidad organizacional se creara un área de trabajo donde tendrán las siguientes carpetas:

i. **Confidencial**.- Es información crítica y solamente podrá ser conocida al interior de la entidad, toda vez que el conocimiento externo de la misma, podrá ocasionar efectos negativos sobre esta.
ii. **Restringida**.- Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información, para estricto cumplimiento de sus funciones.
iii. **Publica**.- Podrá ser utilizada por todos los colaboradores directos de COOTRADIAN y por los temporales, Contratistas y/o terceros de COOTRADIAN

Se deben aplicar los principios de necesidad de saber y de menor privilegio posible. Esta información de igual manera, será respaldada automáticamente todos los días y en línea por la Jefatura de Tecnología y Sistemas de Información.

4.2.2 La Información Confidencial no puede ser distribuida sin las autorizaciones respectivas.

4.2.3 La retención, backups, custodia y destrucción de la Información confidencial, debe estar cubierta por políticas específicas de uso y manejo de información catalogada, definidas por cada Unidad dueña de la información.

4.2.4 La información Restringida, debe ser protegida de acuerdo con los parámetros definidos en uso y manejo de información catalogada, definida por cada Unidad dueña de la información.

4.2.5 La Información Confidencial, no debe ser de conocimiento de personas no autorizadas, ya que es crítico para COOTRADIAN y pone en riesgo la operación y objeto social de la compañía.

POLÍTICAS PARA EL CONTROL DE HARDWARE

SIS-PO-07	
OBJETIVO	Dar a conocer las políticas relacionadas con la administración y control del Inventario de Hardware y Software de COOTRADIAN
ALCANCE	A nivel Nacional para todos los equipos y software que han sido adquiridos y asignados directamente a colaboradores de la compañía, los cuales están dentro de los activos de la empresa, además el hardware y software en poder de terceros o intermediarios, que no hacen parte de los activos de COOTRADIAN

DESARROLLO DE LA POLÍTICA

1. DEFINICIONES

1.1 Software: Es el conjunto de instrucciones electrónicas que indican al PC que es lo que tiene que hacer. Son los programas usados para dirigir las funciones de un sistema de computación o un hardware.

1.2Inventario: Se refiere al conjunto de partes de equipos de cómputo o suministros almacenados para posteriormente ser utilizados.

1.3 Equipo de Cómputo: Es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas, realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

1.4 Hardware: Es el conjunto de elementos materiales que constituyen el soporte físico de un equipo de computo.

2.1 Políticas Generales:

2.1.1 Se consideran Equipos de cómputo y Software de COOTRADIAN, aquellos equipos y software que han sido adquiridos y asignados directamente a colaboradores de la compañía, los cuales se encuentran dentro de los activos de la misma.

2.1.2 La Jefatura de Tecnología y Sistemas de Información es responsable de la administración, manejo y control de los inventarios actualizados de los equipos de la compañía.

2.1.3 El Coordinador de Infraestructura Tecnológica debe informar a la Jefatura de Tecnología y Sistemas de Información los movimientos de activos que se realicen.

2.2 Políticas Específicas:

2.2.1 Todo equipo que se adquiera por parte de la Compañía, debe venir acompañado con la garantía del mismo y una copia de la Orden de Compra.

2.2.2 La Jefatura de Tecnología y Sistemas de Información, es el ente encargado de hacer levantamiento de información de inventarios y de mantenerlo actualizado.

2.2.3 Para los clientes de COOTRADIAN, el manejo de inventarios será actualizado por el personal de la Jefatura de Tecnología y Sistemas de Información, con el fin de ubicar la tecnología existente en cada cliente de negocios o intermediario, para posibles problemas presentados, cambios, ampliaciones, adiciones y/o retiros de equipos de cómputo. (estos equipos no representan activos fijos de la compañía).

2.2.4 La Jefatura de Tecnología y Sistemas de Informaciónes el único autorizado para realizar cambios de configuración de equipos, retiro e instalación de equipos de cómputo, con previa autorización del Coordinador de Infraestructura Tecnológica de COOTRADIAN, para el control centralizado de los mismos.

2.2.5 El Coordinador **de Infraestructura Tecnológica** debe actualizar en el control de inventarios cualquier adición, retiro, actualización, de equipo de cómputo y/o software, inmediatamente esta actividad se realice.

2.2.6 Los inventarios deben ser actualizados de acuerdo a las solicitudes presentadas por los usuarios y/o servicios requeridos, compras realizadas por COOTRADIAN, deben ser controladas con el inventario de equipos de cómputo y/o software, relacionando al usuario a quien será asignado el equipo y realizando el acta de entrega formal.

2.2.7 Los reportes de inventarios deben ser manejados bajo el esquema de informes de gestión, entregados por el Coordinador **de Infraestructura Tecnológica** a la Jefatura de Tecnología y Sistemas de Información, para el control de los mismos.

2.2.8 Se debe realizar una auditoría interna de los cambios reportados por la Jefatura de Tecnología y Sistemas de Información, verificando el movimiento de Hardware y Software efectuado, teniendo en cuenta:

- Los equipos que han sido solicitados temporalmente o en modalidad de arriendo, los cuales, una vez cumplido el tiempo determinado de préstamo, la Unidad de Tecnología deberá, retirar mediante el formato de movimiento de equipos lo siguiente: confirmar el perfecto estado del mismo y actualizando el control de inventarios, con el fin de establecer un control de los mismos. Es responsabilidad de la Jefatura de Tecnología y Sistemas de Información, velar por el cumplimiento legal del software usado durante el periodo de arrendamiento.

- Los equipos que han sido reportados por parte del centro de reparaciones del proveedor de Mantenimiento, con la indicación que se les debe dar de baja, porque su reparación supera las 2/3 partes del valor total del mismo.

2.2.9 El control para la adición y/o retiro de partes de equipos de cómputo, debe realizarse previo requerimiento de las claves de seguridad de los equipos de cómputo. Para las sucursales fuera de la ciudad, los responsables de suministrar las claves de seguridad de equipos de cómputo son los Directores de la oficina quienes deben exigir el diligenciamiento total del formato.

2.2.10 Las órdenes de salida de equipos de cómputo y sus partes, pueden ser autorizadas, únicamente por el Coordinador de Infraestructura Tecnológica. Por cualquier motivo, sino se encuentra la persona autorizada, podrá autorizar el Responsable de Seguridad de la Información, con Visto Bueno del Auxiliar Operativo de Sistemas, mediante el "Formato de Orden de Salida de Equipos de cómputo y partes".

2.2.11 En la recepción del edificio de COOTRADIAN debe existir una lista de personas autorizadas para retirar los equipos de las instalaciones.

2.2.12 Los equipos de cómputo de propiedad de COOTRADIAN que se encuentren en manos de terceros no deberán ser movidos, ni trasladados del sitio donde se encuentran ubicados e instalados, para cumplir la labor para la que fueron asignados.

2.2.13. El computador deberá permanecer en todo momento con la guaya entregada junto con el equipo, durante las noches o ausencias prolongadas, el equipo deberá quedar almacenado bajo llave en los respectivos cajones de los escritorios, evite sacar el computador de las oficinas de COOTRADIAN. Si no es estrictamente necesario.

2.2.14 El colaborador que saque de las oficinas de COOTRADIAN el equipo portátil, deberá comprometerse por el buen manejo del equipo en todo momento, para evitar que se pierda o que se extraiga de él información confidencial de la Compañía.

2.2.15 Los colaboradores a los cuáles se les ha asignado un computador portátil, deberán entender la responsabilidad que esto implica, por lo tanto, en caso de pérdida del equipo

atribuible al usuario o por irresponsabilidad de este, COOTRADIAN podrá hacer efectivo al funcionario el pago del valor correspondiente al deducible del seguro.

2.2.16 El manejo en los equipos portátiles de la información crítica o catalogada como confidencial, se debe realizar de acuerdo a la política de "Catalogación de la Información".

2.2.17 Está expresamente prohibido, el ingreso de equipos de cómputo personales a las instalaciones de la compañía, con el fin de salvaguardar la seguridad de la información.

POLÍTICA DE USO DE CORREO ELECTRÓNICO

SIS-PO-08	
OBJETIVO	Proteger los datos e información crítica de COOTRADIAN mediante el establecimiento de políticas y responsabilidades que permitan realizar un uso adecuado del correo electrónico.
ALCANCE	La presente Política es de aplicación institucional y su carácter es obligatorio para todos los colaboradores o terceros que presten los servicios a COOTRADIAN, que por requerimientos de las funciones que desempeñen dentro de la empresa requieran contar con el servicio de Correo Electrónico en la red de COOTRADIAN, para fines de intercambio o consulta de información, soporte o servicios hacia clientes o proveedores.

DESARROLLO DE LA POLITICA
1. POLÍTICAS Esta política es enunciativa toda vez que no abarca todos los aspectos en los cuales se pueda incurrir. En este orden de ideas, toda actividad que viole o sea contraria a la ley, las regulaciones o las normas aceptadas de la comunidad de Internet, o que perjudique el desempeño de la red, la imagen o las relaciones con los clientes de COOTRADIAN, así no se mencionen o se incluyan dentro de este documento, se entenderán comprendidas en este, dado que su fin es preservar la integridad y disponibilidad de correo electrónico, Internet y de sus usuarios. **Generales**

El correo electrónico es el medio de comunicación, autorizado por COOTRADIAN , para el intercambio de información entre los colaboradores de diferentes Unidades y de estos con los clientes y proveedores de servicios para COOTRADIAN

El correo electrónico es un instrumento o herramienta de trabajo, cuya propiedad corresponde a COOTRADIAN y cuyo uso se otorga a los colaboradores vinculados directamente con COOTRADIAN.

En algunas situaciones puntuales, se otorgará el permiso de la utilización de correo electrónico a los Terceros que presten servicios a favor de COOTRADIAN, por razón de su labor, con las restricciones a que haya lugar.

1.1. Selección de un ambiente de Correo Electrónico

Reconociendo las ventajas de un servicio de correo electrónico para la compañía y sus colaboradores, COOTRADIAN, a través de la Jefatura de Tecnología y Sistemas de Información, debió determinar un ambiente de correo electrónico estandarizado que sea además soportado por la Jefatura de Tecnología y Sistemas de Información. Los factores que se tuvieron en cuenta para la determinación son:

- Escalabilidad del sistema de Correo electrónico.
- Integración con los ambientes estándar de escritorio.
- Compatibilidad con otros sistemas de Correo electrónico en Internet.
- Alto nivel de Seguridad y administración.
- Interface de acceso vía navegador Web (P.ej. Internet Explorer).
- Intuitivo y de fácil entendimiento.

1.2. Acceso al ambiente de correo electrónico de la Compañía

- El acceso al ambiente de correo electrónico de la compañía debe estar disponible para todos sus colaboradores de acuerdo a los principios y procedimientos detallados en esta sección.
- El acceso estará disponible dentro de la Compañía y en forma remota.
- Los colaboradores de la Compañía, deben estar motivados y darle un buen uso al servicio de

correo electrónico. Ahora bien, existen algunos colaboradores que no tienen acceso al correo electrónico regularmente, por tanto, se debe contar con otros medios para su localización.

1.3. Responsabilidades de uso

Cada persona que tenga acceso al Correo electrónico proveído por la Compañía, tiene la responsabilidad de usarlo de acuerdo al beneficio común, así como los principios, procedimientos y regulaciones establecidas, para su adecuado uso. Cualquier usuario que le dé un uso indebido a su buzón de correo, le será removida la cuenta o incluso a dar inicio a un proceso disciplinario.

1.4. Del Servicio

- Para permitir que la Jefatura de Tecnología y Sistemas de Información mantenga el buen desempeño y la integridad del correo electrónico de la compañía, los límites de buzón de correo serán definidos por una capacidad de almacenamiento en disco para cada usuario.

- La capacidad de buzón de correo es establecida en 2 TB para todos los usuarios, en el servidor de correo corporativo. El usuario es responsable de mantener su base de datos de correo depurada (Eliminando el correo innecesario y/o Archivando el correo pertinente).

- Es responsabilidad de cada usuario mantener su buzón con capacidad remanente para recibir correos. Por lo menos el **20%** de su capacidad total.

- El almacenamiento adicional para usuarios individuales debe ser solicitado directamente por el Gerente del área correspondiente a la Jefatura de Tecnología y Sistemas de Información. La solicitud será evaluada y ejecutada por la Jefatura de Tecnología y Sistemas de Información, previa aprobación de la Gerencia respectiva.

- No se permite enviar mensajes que contengan más de diez (10) anexos, los cuales a su vez no deben sobrepasar los 25 MB. Se aceptan tamaños superiores solo con fines corporativos y que estén previamente autorizados por el Comité de Seguridad de la Información.

- COOTRADIAN no es responsable de la falla de servicios de terceros.

- COOTRADIAN no se hace responsable ni controla la información suministrada por terceros, no garantiza la veracidad, integridad o calidad de la misma.

- COOTRADIAN no garantiza que los archivos que se transfieren por la red de Internet estén libres de virus, gusanos, caballos de Troya o demás códigos de infección. El usuario es responsable por la generación o recepción de toda la información realizada por este medio.

- Para los mensajes de salida que no puedan ser entregados a su destino por error en la dirección externa o desaparición de ésta, se le notifica al usuario el problema y el estatus.

- Los servicios autorizados por esta política son monitoreados y en cualquier caso, el ejercicio de dichas facultades por parte de COOTRADIAN, no implica respecto del usuario, la vulneración de sus derechos a la intimidad y a la inviolabilidad de la correspondencia.

1.1. Restricciones de uso

- Anunciar, enviar, presentar o transmitir contenido de carácter ilegal, que atente la dignidad del ser humano, que tenga la potencialidad de ser peligroso, que genere pánico económico, social, de salubridad, etc.

- Crear identidades falsas con el propósito de confundir a terceros.

- Enviar correo basura, spam indiscriminado, o **encadenado** no autorizado o consentido previamente por los destinatarios.

- Es un deber de los usuarios de COOTRADIAN utilizar el servicio de correo electrónico de manera adecuada y responsable. El spamming es una actividad ilegal que no es permitida ni tolerada por COOTRADIAN
    - Se define spamming como la acción de enviar correo electrónico SPAM.

    - Se define spammer como aquel que envía correo SPAM.

    - Se define correo SPAM como el envío de cualquier correo electrónico, masivo o no, a personas (usuarios de COOTRADIAN y usuarios de otras redes) que incluyen temas tales como pornografía, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

  Cuando se habla de envío masivo y no de correo electrónico, COOTRADIAN lo entiende como el envío de uno o más correos a usuarios que no lo han solicitado, independientemente que las direcciones de correo electrónico de los destinatarios, se encuentren en el campo PARA, CC o BCC, del correo electrónico generado.

- El colaborador debe obligarse a impedir fugas de información confidencial o secreta o evitar la sustracción o utilización indebida de la documentación en información clasificada o

confidencial a la cual tiene acceso y que le corresponde custodiar por razón de su cargo o función.

- Esta estrictamente prohibido, realizar afirmaciones que produzcan pánico general, cualquiera sea su intención (económico, social, político o natural).

- Esta estrictamente prohibido utilizar este servicio para hostigamiento o provocaciones de cualquier índole, para la transmisión de material obsceno o pornográfico, así como para el envío de cartas o mensajes que por su contenido puedan degenerar en cadenas de correo.

- Debe existir neutralidad y transparencia del personal de la Empresa durante los procesos electorales, por lo cual está prohibido realizar proselitismo político influyente y cualquier actividad política partidaria o electoral en la Compañía y con los recursos de la Compañía.

- Está estrictamente prohibido el envío de información confidencial, omitiendo buenas prácticas para mantener la confidencialidad e integridad de esta información.

- Está estrictamente prohibido el acceso a este servicio a través de la cuenta de un tercero, así como el préstamo de claves de acceso. Se considera una falta grave el mal uso de las claves de acceso y ocasionará la suspensión definitiva del mismo.

- El acceso al servidor de correo desde una conexión pública (acceso remoto) por medio de un Agente de Correo (p.ej. Outlook) está limitado a descargar y ver todo el contenido de su buzón de correo. En caso de tener que enviar un correo es indispensable hacerlo vía Webmail.

- Los correos que se generen deben, en lo posible, ser cortos, no tener saludos efusivos y sólo remitir copias a los usuarios que realmente lo requieran. Al final del mensaje se debe registrar el nombre de quien lo escribe, de acuerdo con el modelo de firma autorizado por la Compañía.

Uso de dispositivos Móviles

- Solo se permitirá habilitar las funcionalidades de sincronización de correo, contactos y agenda de este tipo de dispositivos a las directivas, cargos medios y personal que autorice la Gerencia respectiva por motivos de sus funciones laborales.

- Estos dispositivos deben tener una contraseña de arranque.

- Estos dispositivos deben tener seguridad de cifrado, y bloqueo automático en caso de reporte de perdida.

- Es responsabilidad del usuario velar por la seguridad de la información confidencial contenida en los dispositivos.

- En cualquier momento estos dispositivos pueden ser revisados por el Responsable de Seguridad de la información para validación de las normas mínimas de seguridad enunciadas en esta política.

CONSECUENCIAS POR EL MAL USO DE LOS SERVICIOS

Cuando el colaborador incumpla cualquier disposición de estas políticas sobre el uso de los servicios de tecnología informática y telecomunicaciones de COOTRADIAN , se dará inicio al respectivo proceso disciplinario, para lo cual, se tendrá en cuenta el procedimiento y las sanciones previstas en el Reglamento Interno de Trabajo y demás ordenamientos internos, según el usuario del que se trate. Lo anterior, sin perjuicio de las sanciones contempladas en las normas legales vigentes.