MANUAL DE SEGURIDAD DE LA INFORMACIÓN

Revisó: Comité de Seguridad de la Información.

Aprobó: Gerencia

TABLA DE CONTENIDO

INTRODUCCIÓN

Las empresas modernas, cada vez más dependientes de la tecnología, enfrentan una serie de riesgos por cuenta de las herramientas que apoyan su negocio. Virus, spyware, 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.

1. MARCO NORMATIVO

Las instrucciones de que trata el presente documento, cumplen con lo contemplado en el capítulo IV, Título IV de la Circular Básica Contable y Financiera de la Supersolidaria sobre el Sistema de Administración de Riesgo Operativo.

2. DEFINICIONES

Para efectos de la presente Norma, se establecen las siguientes definiciones:

2.1. Acción resolutiva

Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.

2.2. Activo de información

Conocimiento o datos que tienen valor para la organización o el individuo.

2.3. Amenaza

Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.

2.4. Confidencialidad

Considera que la información no se pone a disposición ni se revela a personal o a entidades no autorizadas.

2.5. Control

Medida o acción que modifica un riesgo para prevenir su materialización.

2.6. Disponibilidad

Posibilidad de que la información debe estar accesible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

2.7. Gobierno de seguridad de la información

Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

2.8. Incidente de Seguridad

Se define como un evento que atenta contra la confidencialidad, integridad y/o disponibilidad de la información y los recursos tecnológicos de la organización.

2.9. Integridad

La información debe ser precisa, coherente y completa desde su creación hasta su destrucción, debe ser inalterada ante accidentes o intentos maliciosos, siempre se debe prevenir modificaciones no autorizadas de la información.

2.10. Nivel de riesgo

Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.

2.11. Probabilidad

Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.

2.12. Políticas de seguridad:

Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por el consejo de administración.

2.13. Riesgo residual:

Es el riesgo que queda después de aplicar los controles al riesgo identificado.

2.14. Seguridad de la información:

Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización.

2.15. Servicios de computación en la nube:

Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios.

2.16. **Vulnerabilidad:**

Debilidad de un activo o control que puede ser explotado por una o más amenazas.

3. ROLES Y RESPONSABILIDADES

El consejo de administración u órgano que haga sus veces en la organización solidaria, será quien apruebe la política de seguridad de la información y sus modificaciones, considerando como mínimo, las siguientes actividades:

3.1. Consejo de Administración

a. Definir y promover la dirección estratégica para la seguridad de la información.

b. Proporcionar los recursos para la adecuada implementación de la seguridad de la información.

c. Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.

d. Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.

e. Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.

f. Velar por la disponibilidad de los recursos y su uso apropiado.

g. Designar los responsables de la implementación del sistema de seguridad de la información.

h. Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.

i. Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.

j. Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio.

k. Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

3.2. Gerente

a. Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos por el consejo de administración.

b. Velar por la implementación de la política de seguridad de la información.

c. Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.

d. Velar por la disponibilidad de los recursos y su uso apropiado.

e. Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información.

f. Velar por la designación de los responsables de la implementación de la política de seguridad de la información.

g. Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

3.3. Comité de Seguridad de la información.

a. Definir y mantener una política de seguridad de la información, incluyendo procedimientos y prácticas para proteger los datos sensibles.

b. Supervisar y evaluar continuamente la implementación de medidas de seguridad de la información, incluyendo la realización de auditorías y pruebas de penetración.

c. Identificar y evaluar continuamente los riesgos potenciales para la seguridad de la información, y desarrollar estrategias para mitigarlos.

d. Asesorar y guiar a la dirección y empleados en cuestiones relacionadas con la seguridad de la información, incluyendo la sensibilización y la formación.

e. Establecer y mantener un plan de respaldo y recuperación en caso de desastres, y asegurarse de que esté regularmente revisado y actualizado.

f. Investigar y responder a incidentes de seguridad de la información, y coordinar con las autoridades apropiadas en caso de una violación de seguridad importante.

g. Monitorear y cumplir con todas las leyes y regulaciones relevantes relacionadas con la privacidad y la seguridad de la información.

3.4. Coordinador de sistemas

a. Planificar y coordinar la implementación de nuevos sistemas y tecnologías para mejorar la eficiencia y la seguridad de la información.

b. Supervisar y mantener los sistemas y redes existentes, incluyendo la solución de problemas y la realización de actualizaciones y mejoras.

c. Evaluar continuamente la infraestructura de tecnología de la información y identificar oportunidades de mejora.

d. Coordinar con proveedores externos y contratistas para garantizar un servicio de alta calidad y una solución rápida a los problemas.

e. Asesorar y guiar a los usuarios en cuestiones relacionadas con la tecnología de la información, incluyendo la resolución de problemas y la formación.

f. Monitorear y cumplir con los estándares y regulaciones relevantes en materia de seguridad de la información y privacidad.

g. Desarrollar y mantener planes de contingencia y recuperación en caso de desastres tecnológicos, y asegurarse de que estén regularmente revisados y actualizados.

3.5. Revisoría Fiscal

a. Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular.

b. Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del sistema de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.

c. Informar los resultados de la evaluación de la seguridad de la información al consejo de administración.

3.6. Recursos humanos

Las organizaciones deben tener definidos claramente los términos y condiciones de los cargos asociados a la seguridad de la información entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y

los trabajadores en general, respecto a las funciones y responsabilidades en la seguridad de la información.

Adicionalmente, es conveniente contar con un programa de concientización/educación sobre la seguridad de la información extendida a directivos y trabajadores, para lo cual será necesario:

a. Proveer toda la información a los funcionarios sobre la postura, estrategias y políticas de seguridad de la información de la organización.

b. Implementar un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial, por parte de los trabajadores, el cual deberá ser informado a estos desde el proceso de inducción.

c. Se deberán tener en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias y despidos.

4. OBJETIVOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a. Tener comprensión de las amenazas, las vulnerabilidades, y el perfil de riesgo de la organización.

b. Tener entendimiento de la exposición al riesgo y las posibles consecuencias para el negocio.

c. Crear conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias de materialización.

d. Definir e implementar estrategias organizacionales adecuadas para la mitigación de riesgos para obtener consecuencias aceptables.

e. Fijar la atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual.

f. Conservar información documentada del proceso de gestión de riesgos de seguridad de la información.

4.1. Sistema de Seguridad de la información

Las organizaciones deberán contar con políticas que identifiquen el contexto y los objetivos propios, atendiendo como mínimo lo siguiente:

a. Descripción

El proceso de descripción de las políticas de seguridad de la información, implica que bajo un lenguaje conciso y de fácil comprensión, se identifiquen e incorporen los temas propios de seguridad, normativa aplicable, tipo de información sensible, identificación de la clasificación de la información, responsables y niveles de autorización.

b. Revisión

El proceso de revisión debe contemplar la aplicación de actividades de retroalimentación como soporte de conocimiento que permitan la socialización y la verificación del cumplimiento de las políticas de seguridad, alineadas con los objetivos de la organización solidaria.

c. Aprobación

Este proceso está a cargo del consejo de administración o, quien haga sus veces, en la organización, quien emitirá la aprobación de las políticas del Sistema de Seguridad de Información y establecerá las instrucciones para su puesta en marcha y cumplimiento.

d. Publicación

Cumplidos los procesos de descripción, revisión y aprobación, la organización vigilada dará a conocer las políticas de seguridad de la información, las cuales deberán ser publicadas a través de los medios de comunicación que habitualmente utiliza, siendo necesario que se apliquen estrategias que faciliten su difusión y su contenido por todos y cada uno de los integrantes de las organizaciones.

e. Evaluación

La organización solidaria deberá aplicar evaluaciones de conocimiento al personal, garantizando que las políticas son leídas y se aplican de acuerdo a lo establecido.
Actualización.

El desarrollo de la Seguridad de Información debe considerarse como un proceso de mejora continua, por lo cual, al aplicar los controles de seguridad bajo parámetros previamente establecidos para su medición, debe generar como resultado los aspectos a corregir, los cambios que se deben realizar o, la identificación de nuevos riesgos.

De igual forma, el resultado de las evaluaciones y verificaciones que evidencien el recurrente incumplimiento a las políticas, la recepción de sugerencias por las partes interesadas y la oportunidad de cambios tecnológicos al interior de la organización

solidaria, le permitirán a esta tomar decisión en relación con la necesidad de llevar a cabo procesos de actualización de dichas políticas.

5. RECURSOS

5.1. Presupuesto

El presupuesto de COOTRADIAN, contempla los activos de información involucrados y los recursos que aseguren la función de seguridad de la información, las herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua.

5.2. Competencia

COOTRADIAN debe procurar que los responsables de la seguridad de la información cuenten con la competencia necesaria para gestionar los riesgos asociados, evaluar la eficacia de las acciones tomadas y garantizar la información documentada.

5.3. Comunicación

La comunicación es especialmente importante entre todas las partes interesadas dentro de las cadenas de suministro, por lo que el Sistema de Seguridad de Información debe proporcionar un medio para comunicar los requisitos exigidos, entre los responsables de la entrega de productos y servicios esenciales de la organización.

5.4. Información documentada

El modelo de seguridad de la información de la organización vigilada debe incluir la información documentada requerida por esta norma, considerando los siguientes componentes:

5.4.1. Principios de seguridad de la información

El consejo de administración tiene la responsabilidad de aprobar una política general de seguridad de la información, la cual debe estar disponible para ser entregada a los organismos de vigilancia y control, teniendo en cuenta que:

a. Esté adecuada al propósito de la organización vigilada.

b. Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.

c. Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información.

d. Incluya el compromiso de mejora continua del sistema de seguridad de la información.

e. Esté disponible como información documentada.

f. Se comunique dentro de la organización vigilada

g. Esté disponible para las partes interesadas, según sea apropiado.

5.4.2. **Otra información documentada**

El modelo de seguridad de la información de la organización vigilada, debe estar acompañado por otro tipo de información documentada como:

a. Procedimientos de seguridad.

b. Instructivos o guías técnicas.

5.4.3. **Creación y actualización de la información documentada**

Cuando se crea y actualiza información documentada del sistema de seguridad, la organización vigilada debe asegurarse de que sea apropiado e incluya:

a. La identificación y descripción.

b. El formato y sus medios de soporte.

c. La revisión y aprobación con respecto a la idoneidad y adecuación.

5.4.4. **Control de la información documentada**

La información documentada requerida por el sistema de seguridad de la información, se debe controlar para asegurarse de que esté disponible, adecuada para su uso y esté protegida adecuadamente, entre otros, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad.

El control debe efectuarse sobre la distribución, acceso, recuperación y uso de almacenamiento y preservación, incluida la preservación de la legibilidad, control de cambios, retención y disposición.

6. REQUERIMIENTOS DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

En desarrollo de los criterios de seguridad para los medios tecnológicos y considerando los canales de distribución utilizados, las cooperativas deberán cumplir, como mínimo, con los siguientes requerimientos:

a. Disponer de hardware, software y equipos de telecomunicaciones que mitiguen las amenazas del sector, y crear procedimientos y controles necesarios que permitan la prestación de los servicios y el manejo de la información, en condiciones de seguridad y calidad.

b. Gestionar la seguridad de la información bajo un Modelo de Seguridad y Privacidad de la Información.

c. Gestionar con sus tarjetahabientes estándares de seguridad tales como PCI-DSS.

d. Gestionar mecanismos para el envío de información a sus asociados, tales como: certificaciones, extractos, notificaciones, sobreflex, entre otros, así como los medios (tarjetas débito y crédito, chequeras, etc.) bajo medidas de seguridad. Cuando la información que la organización remite a sus asociados sea de carácter confidencial y se envíe como parte o adjunta a un correo electrónico, ésta deberá estar cifrada.

e. Garantizar, de manera segura, el registro de las direcciones IP y los números de los teléfonos fijos y móviles desde los cuales operará. La entidad podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.

f. Todas las conexiones a aplicaciones de terceros deben estar en mecanismos seguros de conexión como son VPN, canales exclusivos, con el registro de IP por parte de entidades para evitar acceder desde lugares remotos sin la debida seguridad y/o autorización pertinente.

6.1. Controles criptográficos

a. Los sitios web creados para el procesamiento de la información del negocio, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país.

b. Las comunicaciones con terceras partes para la prestación de servicios del negocio, deben utilizar mecanismos de encriptación fuertes.

c. Se deben utilizar herramientas que cuenten con algoritmos de encriptación en el almacenamiento de la información sensible o crítica en archivos, así como las claves de usuarios a los sistemas de información.

d. Protección contra códigos móviles o maliciosos

e. Se debe mantener instalado, en los equipos de la organización, software antivirus los cuales serán actualizados constantemente por parte del área encargada.

f. Evitar o restringir el intercambio de CD´s, memorias tipo USB y otros medios removibles de origen desconocido o, si fuere necesario, someterlos a la revisión del antivirus instalado en el disco antes de su utilización.

g. Restringir el uso de los equipos por parte de personas ajenas a las actividades propias de la organización.

h. En el caso de los archivos comprimidos bajo el formato ZIP o cualquier otro tipo de archivo que fueron descargados por Internet o por correo electrónico, deberán ser revisados por el antivirus inmediatamente después de haber sido desempaquetados y antes de ser ejecutados.

6.2. Intercambio de información

a. No estará permitido intercambiar información con entidades externas sin la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.

b. Cuando se envié información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.

c. Los empleados de las organizaciones y de las empresas aliadas deben estar cubiertos con acuerdos de confidencialidad y, por lo tanto, serán responsables de la entrega de información no autorizada.

d. En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.

e. La información sensible disponible al público a través de sitios web, debe estar protegida por sitios seguros y, adicionalmente, con usuario y clave de acceso.

f. La comunicación con entidades externas para el intercambio de información crítica se debe hacer a través de canales dedicados, con mecanismos de

seguridad, como son VPN o webservices y debe ser configurado por personal de la organización solidaria.

g. La información que viaja entre las oficinas y los sitios centrales de las entidades, deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Cooperativas de ahorro y crédito, el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de Gateway, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las organizaciones deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

h. Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.

i. En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

6.3. Respaldo de la información

A toda la información que se encuentra alojada en los servidores y equipos de cómputo, se le debe garantizar respaldo periódicamente de acuerdo con los procedimientos establecidos, con el fin de contar con la información en caso de ser requerida por alguna eventualidad y se tendrá en cuenta que:

a. Las copias de seguridad deben estar enfocadas a los datos, sistemas y programas, servidores, equipos de escritorio, portátiles, red, sistemas de control, sistemas de seguridad, entre otros.

b. Debe garantizar que los medios de respaldo están físicamente protegidos y asegurados al menos al mismo nivel que los datos operacionales.

c. Las copias de seguridad se deben almacenar en ubicaciones adecuadas, protegidos contra desastres físicos y acceso indebido.

d. Se debe implementar un procedimiento para probar, de forma regular, las copias generadas y así garantizar su integridad y funcionalidad al momento de una restauración.

6.4. Sincronización de Relojes

Todos los equipos tanto, servidores, switches, equipos de cómputo, circuito cerrado de cámaras de vigilancia - CCTV, y todos aquellos dispositivos tecnológicos que se tienen en la organización se deben sincronizar a la hora legal colombiana, sin excepción alguna. Se debe garantizar, por medio de seguimiento y con el respectivo indicador, el cumplimiento de la correcta sincronización de la hora según lo expuesto en el numeral 14, del artículo 6, del Decreto 4175 de 2011, con apoyo del Instituto Nacional de Metrología de Colombia (http://horalegal.inm.gov.co).

6.5. Controles de Acceso

Se aplica a todas las formas de acceso a las instalaciones de la organización y para aquellas áreas definidas como "áreas críticas", debido a su relación con datos confidenciales y de interés para el negocio, así:

a. El acceso a las instalaciones que opten por el uso de aplicaciones por medio de software de control de acceso biométrico o tarjeta, debe definir sus responsables y el debido tratamiento de datos personales, conforme a lo dispuesto en la Ley 1581 del 2012, la cual trata del uso de datos sensibles según su clasificación.

b. El acceso de todo el personal (incluyendo contratistas y visitantes) a los Datacenter y Centros de Cableado, debe estar restringido y sólo pueden acceder a través de la autorización del correspondiente funcionario.

c. Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y, en general, todos los dispositivos de los Datacenter, centros de cableado y los armarios (Racks), deben permanecer cerrados.

d. Si se requiere el uso de cámaras de video (CCTV) u otros mecanismos de control de acceso (proximidad o control de acceso biométrico) para supervisar el acceso físico de personas a áreas críticas o que resguardan información confidencial, deben generar su respectivo procedimiento de tratamiento de copias de seguridad a menos que la ley u otras regulaciones requieran un tiempo superior de custodia.

e. Se deben implementar controles físicos que impidan el acceso a conexiones o puntos de red de acceso público. Esto incluye limitar el acceso físico a los puntos de acceso inalámbricos, dispositivos de telecomunicaciones, manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.

6.6. Tele-Trabajo (Home Office)

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. Esto incluye el uso de teléfonos móviles, tabletas y similares fuera de las instalaciones de la organización, por lo cual:

a. El acceso remoto a los servidores que se encuentran fuera de las instalaciones de la organización, debe estar autorizado por el comité de riesgos o quien delegue la gerencia general.

b. Las áreas de trabajo remoto que autorice la organización fuera de su sede principal, deben cumplir con todas las políticas y controles del sistema de seguridad definido para proteger la información que viaje en ellos.

c. El personal de infraestructura de informática y tecnología son responsables de proporcionar el servicio de acceso.

6.7. Acceso a las redes WIFI

a. El acceso a las redes inalámbricas por parte de los empleados, a través de WiFi, se debe realizar con autenticación usuario y contraseña, independientemente de la herramienta que se quiera utilizar para controlar el acceso.

b. Las redes WiFi para asociados o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas.

6.8. Aspectos no permitidos

Los aspectos no permitidos deben quedar contenidos en políticas, principios o procedimientos, manuales y ser de conocimiento por todos los funcionarios de la organización, entre ellos:

a. Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.

b. Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.

c. Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.

d. Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.

e. Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella. Tampoco se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.

f. Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.

g. Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

6.9. Prestación de servicios por terceras partes

Cuando la organización requiera la contratación de prestación de servicios por terceras partes debe, como mínimo:

a. Firmar el documento de acuerdo de confidencialidad antes de iniciar la prestación del servicio.

b. Elaborar los contratos o acuerdos de prestación de servicios donde se especifiquen claramente las condiciones.

c. Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.

d. La organización realizará auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

6.10. Gestión de Incidentes de Seguridad

Existen varias categorías de incidentes de seguridad que se pueden llegar a presentar, dentro de las cuales se encuentran:

a. Acceso no autorizado: Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

    i. Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.

ii. Robo de información
iii. Borrado de información
iv. Alteración de la información
v. Intentos recurrentes y no recurrentes de acceso no autorizado
vi. Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación

b. Código malicioso: Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la organización. Son parte de esta categoría:

i. Virus informáticos
ii. Troyanos
iii. Gusanos informáticos

c. Denegación del servicio: Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

i. Tiempos de respuesta muy bajos sin razones aparentes.
ii. Servicio(s) interno(s) inaccesibles sin razones aparentes
iii. Servicio(s) Externo(s) inaccesibles sin razones aparentes

d. Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular. Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la organización y comprende:

i. Sniffers (software utilizado para capturar información que viaja por la red)
ii. Detección de Vulnerabilidades

e. Mal uso de los recursos tecnológicos: Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y comprende:

i. Mal uso y/o Abuso de servicios informáticos internos o externos
ii. Violación de las normas de acceso a Internet
iii. Mal uso y/o Abuso del correo electrónico de la organización
iv. Violación de las Políticas, Normas y Procedimientos de Seguridad Informática establecidas para proteger la información

Es deber de todas las organizaciones reportar un incidente de seguridad tan pronto lo detecte o se sospeche de él, aplicando el procedimiento interno definido para tal efecto.

Adicionalmente, si estos desencadenan en fraudes para la organización se deberán poner en contacto con las entidades encargadas para la investigación y sanción de estos hechos denominados delitos informáticos, así como informar tal situación a la Superintendencia de la Economía Solidaria.

6.11. Divulgación de Información

Diseñar procedimientos para dar a conocer a los asociados, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales.

6.12. Inventario de activos

Las organizaciones deberán contar con un inventario de activos de la información, especificando, como mínimo, los siguientes aspectos:

- Datos digitales
- Información impresa
- Software
- Infraestructura
- Servicios de información y proveedores de servicios
- Seguridad física
- Relaciones comerciales
- Responsables de los activos.

Se deben identificar los activos asociados con información e instalaciones de procesamiento de información.

Así mismo, se deberá contar con un proceso y procedimiento detallado para mantener el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI.

6.13. Datafono

a. La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos cumpliendo con los estándares PCI-DSS.

b. Los administradores de tecnología son los responsables de validar automáticamente la autenticación del datáfono que se intenta conectar a ellos, así como garantizar que los canales de comunicación se encuentren con los debidos controles criptográficos descritos en el presente documento.

c. Establecer procedimientos que le permitan identificar los responsables de los datáfonos en los establecimientos comerciales y confirmar la identidad de los funcionarios autorizados para retirar o hacerles mantenimiento a los equipos.

d. Velar porque la información confidencial de los asociados y usuarios no sea almacenada o retenida en el lugar en donde los datafonos estén siendo utilizados reduciendo la posibilidad que terceros puedan ver la clave digitada por el asociado o usuario.

6.14. Transacciones por Internet

Las organizaciones que ofrezcan la realización de operaciones por Internet deberán cumplir como mínimo lo siguiente:

a. Implementar los controles descritos en los algoritmos y protocolos necesarios para brindar una comunicación segura.

b. Realizar, como mínimo dos (2) veces al año, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional, esto debe ir acompañado de su respectivo documento de control de cambios.

c. Promover y poner a disposición de sus asociados mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.

d. Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

e. Informar al asociado, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.

f. Implementar mecanismos que permitan a la organización verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS1.

[1] El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space) consiste en resolver las peticiones de asignación de nombres.

6.15. **Análisis de Vulnerabilidades**

COOTRADIAN deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes aspectos:

a. Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

b. Generar, de manera automática, por lo menos dos (2) veces al año, un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos (2) años deben contener sus planes de acción y sus remediaciones.

c. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

d. Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.

e. Los informes generados deberán tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

6.16. **Instalaciones y suministros**

La organización debe proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. Por lo tanto, deberá contar con lo siguiente:

a. Un sistema de UPS[2] para proporcionar una potencia adecuada, confiable y de alta calidad para abarcar todos los equipos esenciales durante un período de tiempo suficiente.

b. Un plan de mantenimiento y pruebas para los UPS y generadores.

c. Contar con una red de suministro eléctrico redundante.

d. Implementar controles para las pruebas de cambio y así garantizar la no afectación de los sistemas y servicios.

[2] Una UPS (Uninterruptible Power Supply) o sistema de alimentación ininterrumpida, es una fuente de suministro eléctrico que permite brindar energía eléctrica por un tiempo limitado a dispositivos eléctricos/electrónicos en el caso de interrupción eléctrica.

e. Contar con sistemas de aire acondicionado redundantes para controlar entornos con equipos críticos y así mantener una capacidad adecuada de A/C[3] para soportar la carga de calor.

f. Implementar detectores de temperatura.

6.17. Planificación e implementación de la continuidad de la seguridad de la información

La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas. Así mismo, deberá establecer, documentar, implementar y mantener procesos procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

De igual forma, la organización debe verificar, a intervalos regulares, los controles de continuidad de la seguridad de la información establecidos e implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas. Por lo tanto, deberá contemplar los siguientes aspectos fundamentales:

a. Determinar los requisitos de continuidad del negocio.

b. Elaborar un plan de continuidad de negocio.

c. Contar con un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos.

d. Identificar el impacto potencial de los incidentes.

e. Evaluar los planes de continuidad del negocio.

f. Realizar DRP[4] para validar el nivel de respuesta de la organización ante un incidente.

g. Los planes deberán tener plazos definidos para restaurar servicios tras una interrupción.

h. Los planes deberán contar con la identificación y asignación de responsabilidades, la identificación de pérdidas aceptables, la implementación

[3] A/C: esta sigla corresponde a aire acondicionado o sistema de aire acondicionado.

[4] DRP o Plan de Recuperación de Desastres, es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversa índole que puedan dañar su infraestructura tecnológica.

de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares.

i. La planificación de la continuidad deberá ser consistente y debe identificar las prioridades de restauración.

j. Deberá contar con miembros de los equipos de recuperación o gestión de crisis o incidentes, con conocimiento de los planes, estableciendo de forma clara sus roles y responsabilidades.

k. Los controles de seguridad deberán estar adecuados para los sitios de recuperación de desastres remotos.

l. Deberá contar con un método de pruebas del plan de continuidad.

m. Se debe establecer la frecuencia con la que se llevaran a cabo las pruebas.

n. Deberán llevar un registro de evidencias de las pruebas reales efectuadas, junto con sus resultados y planes de mejora.

o. Deberán identificar deficiencias para así remediarlas y posteriormente volverlas a probar hasta que los resultados sean satisfactorios.

6.18. Reutilización o eliminación segura de equipos

La organización debe implementar una política para establecer controles con el propósito de verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.

a. La organización debe evitar que se revele la información almacenada en equipos y dispositivos tras su reasignación o eliminación, mediante el uso de cifrado fuerte o borrado seguro.

b. Llevar un control y registro de cada uno de los medios que se eliminan.

7. POLÍTICAS GENERALES Y BUENAS PRÁCTICAS

a. 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.

b. 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.

c. Los colaboradores de la empresa, que tengan conocimiento de cualquier uso indebido del software, deberán notificar este hecho a la Gerencia o al Responsable de Seguridad de la Información (Coordinador de Sistemas) para que se tomen las acciones del caso.

d. 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 y con la ley 603 de 2000, sus adiciones y modificaciones.

e. COOTRADIAN no permite ni autoriza ningún tipo de copia ilegal de programas o bases de datos, con información sensible propia o de terceros recibida en custodia. De detectarse un incumplimiento, la Gerencia, 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.

f. AUDITORIA.- En cualquier momento el área encargada, efectuará auditorías a los diferentes computadores de la Compañía, con el fin de verificar que no se encuentre software no autorizado ni legalizado.

g. Los componentes de 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, para los cuales se le otorgó el permiso.

Esto significa que:

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

b. La seguridad de los sistemas de computación, incluyendo los datos corporativos, comunicaciones electrónicas y aplicaciones (software), deben estar protegidos todo el tiempo, por lo tanto ningún funcionario debe atentar contra esa seguridad de los recursos los cuales tiene acceso.

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

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

e. 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.

f. Cada colaborador autorizará a las Directivas de COOTRADIAN para acceder y revisar los equipos que tiene asignados 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.

g. 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 Coordinación de Tecnología y Sistemas de Información.

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

La Cooperativa 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:

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

b. 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.

c. 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.

d. 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.

e. 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 y/o asesor legal.

7.2. Bienes y Tiempo de la Compañía

Los bienes tecnológicos 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 de este, evitando la malversación o el robo de los mismos.

Esto significa que:

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

b. 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).

c. 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.

8. 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

Políticas Generales

- 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.

- Todos los equipos de cómputo conectados a la red de la compañía y que se encuentre dentro del dominio COOTRADIAN tienen acceso a Internet.

Políticas Especificas

Políticas de Uso de Acceso a Internet:

- 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.

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

- 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.

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

- 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 Coordinación de Tecnología y Sistemas de 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, para dar inicio al proceso disciplinario y aplicar las sanciones 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, 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 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 Coordinación de Tecnología y Sistemas de Información y con fines de soporte remoto.

- 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.
- 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.

9. 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.

DESARROLLO DE LA POLITICA

Políticas Generales

a. El Software solo podrá ser instalado por el personal de Tecnología de COOTRADIAN , el software no incluido dentro del estándar, deberá ser solicitado únicamente por el Gerente, la Coordinación 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.

b. Toda adquisición de Software que sea necesario para el soporte de actividades de las diferentes áreas será adquirido a través de la Coordinación 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 Coordinación de Tecnología y Sistemas de Información.

c. La Coordinación 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.

d. La Coordinación 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.

e. 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.

10. 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	

Políticas Generales

El personal que no es titular de un computador o 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 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, además 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 Coordinación 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.

11. 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	

Políticas Generales

Los usuarios deben establecer contraseñas acorde con las recomendaciones dadas por la Coordinación 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 (Coordinación 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:

a. Ejecución de programas no autorizados y no avalados por la Coordinación de Tecnología y Sistemas de Información.

b. Violación a la POLÍTICA DE ACCESO A INTERNET.

c. Propagación de un virus desde el computador al cual el usuario está 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.

12. 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

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.

POLITICAS :

Políticas Generales:

- 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.

- 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.

- 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 Coordinación de Tecnología y Sistemas de Información.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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. .

- 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.

- 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.

- 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 Coordinación de Tecnología y Sistemas de Informacióno al Responsable de Seguridad de la Información.

- Ninguna persona diferente a las autorizadas por la Coordinación 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

- 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.

- 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

- 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.

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.

13. 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 cómputo, 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

DEFINICIONES:

- **Información No Clasificada:** Declarada como pública, puede ser libremente entregada a personas no autorizadas sin causar daño a la compañía.
- **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.
- **Información Confidencial:** Es aquella más sensible y que en manos de terceros, puede poner en riesgo el negocio.
- **Información Restringida:** Declarada como secreta y de uso exclusivo de las personas que COOTRADIAN determine como autorizadas.
- **Confidencialidad:** La información de los sistemas, es accedida solo por usuarios autorizados.
- **Integridad**: La información de los sistemas, sólo puede ser creada y modificada por los usuarios autorizados.
- **Disponibilidad**: La información siempre está disponible cuando se necesita.

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

- **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.

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

- **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.

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

- **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.

Políticas Generales:

El dueño de la información, debe asociar cada tipo de información pertinente a su área, en tres niveles de catalogación establecidos así:

• De uso general (Pública).

• Restringida.

• Confidencial.

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.

Políticas Específicas:

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) En la nube de cada computador en la aplicación de google Drive

b) Los computadores involucrados en procesos críticos será respaldada periódicamente por la Coordinación 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 Coordinación 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:

- ✓ **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.
- ✓ **Restringida**.- Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información, para estricto cumplimiento de sus funciones.
- ✓ **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 Coordinación 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.

14. 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

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.

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

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.

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

Políticas Generales:

- 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.

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

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

Políticas Específicas:

- 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.

- La Coordinación de Tecnología y Sistemas de Información, es el ente encargado de hacer levantamiento de información de inventarios y de mantenerlo actualizado.
-
- Para los clientes de COOTRADIAN, el manejo de inventarios será actualizado por el personal de la Coordinación 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).
-
- La Coordinación 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.
-
- 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.

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

- Se debe realizar una auditoría interna de los cambios reportados por la Coordinación 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 Coordinación 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.

- 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.

- 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".

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

- 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.

- 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.

- 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.

- 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.

- 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".

- 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.

15. 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	

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.

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 Coordinación de Tecnología y Sistemas de Información, debió determinar un ambiente de correo electrónico estandarizado que sea además soportado por la Coordinación 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.

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.

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.

Del Servicio

- Para permitir que la Coordinación 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 a la Coordinación de Tecnología y Sistemas de Información. La solicitud será evaluada y ejecutada por la Coordinación 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.

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 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.