1. INTRODUCCIÓN

Para COOUNISAN es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios al sistema de información, garantizando que la información sea protegida en su manejo, procesos y almacenamiento.

Las políticas incluidas en este documento se constituyen como parte fundamental del sistema de gestión de seguridad de la información de COOUNISAN y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

2. OBJETIVO

Garantizar que el sistema informático y los recursos de software de COOUNISAN se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

3. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los empleados, clientes y proveedores que laboren o tengan relación con COOUNISAN, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información.

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la compañía y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en los que los empleados de COOUNISAN o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: son sitios al interior de la compañía donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los Centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, terceros o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: 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.

Guías de clasificación de la información: directrices para catalogar la información de la compañía y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la compañía con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a la compañía.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CD, DVD y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de EMPRESA.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la compañía. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por EMPRESA o de origen externo ya sea adquirido por la Compañía como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características de este, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la compañía.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la compañía (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Consciente de las necesidades actuales, COOUNISAN implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los empleados, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, almacenamiento y recursos de procesamiento de la información de COOUNISAN, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y disponibilidad de la información.

6. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva de COOUNISAN aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la compañía.

La Junta Directiva y la Alta Dirección de la compañía demuestran su compromiso a través de:

•La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
•La promoción activa de una cultura de seguridad.
•Facilitar la divulgación de este manual a todos los empleados de la compañía.
•El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
•La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los empleados, personal externo y proveedores de COOUNISAN. Por tal razón, es necesaria que las violaciones a las Políticas de Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, conforme sea estipulado al Reglamento Interno de Trabajo

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

COOUNISAN establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

8.1.1. NORMAS QUE RIGEN PARA LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Normas dirigidas a: GERENCIA

•La Gerencia debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
•La Gerencia debe promover activamente una cultura de seguridad de la información en la compañía.
•La Gerencia debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los empleados de la compañía y al personal provisto por terceras partes.
•La Gerencia, debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la compañía.

Normas dirigidas a: SISTEMAS

•Debe actualizar y presentar ante la Gerencia las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
•Debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
•Debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
•Debe liderar la generación de lineamientos para gestionar la seguridad de la información de COOUNISAN y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
•Informática debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
•Debe asignar las funciones, roles y responsabilidades para la operación y administración de la plataforma tecnológica de la compañía. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: USUARIOS

•Los empleados y personal provisto por terceras partes que realicen labores en o para COOUNISAN tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8.2. POLÍTICA PARA USO DE DISPOSITIVOS MOVILES

COOUNISAN proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) corporativos que hagan uso de servicios de la compañía.

Así mismo, velará porque los empleados hagan un uso responsable de los servicios y equipos proporcionados por la compañía.

8.2.1. Normas para uso de dispositivos móviles

Normas dirigidas a: SISTEMAS

•Debe investigar y probar las opciones de protección de los dispositivos móviles corporativos que hagan uso de los servicios provistos por la compañía.
•Debe establecer las configuraciones aceptables para los dispositivos móviles corporativos que hagan uso de los servicios provistos por COOUNISAN.
•Debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles corporativos que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
•Debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles corporativos haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
•Debe configurar la opción de borrado remoto de información en los dispositivos móviles corporativos, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
•Debe instalar un software de antivirus en los dispositivos móviles corporativos que hagan uso de los servicios provistos por la compañía.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios deben evitar usar los dispositivos móviles corporativos en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

•Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
•Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles corporativos.

•Los usuarios deben, cada vez que el sistema de sus dispositivos móviles corporativos notifique de una actualización disponible, aceptar y aplicar la nueva versión.
•Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles corporativos asignados.
•Los usuarios deben evitar conectar los dispositivos móviles corporativos asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
•Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles corporativos asignados.

8.3. POLÍTICA PARA USO DE CONEXIONES REMOTAS

COOUNISAN establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la compañía; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

8.3.1. Normas para uso de conexiones remotas

Normas dirigidas a: SISTEMAS

•Debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de COOUNISAN.
•Debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de COOUNISAN.
•Debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
•Debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de COOUNISAN de manera permanente.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de COOUNISAN y deben acatar las condiciones de uso establecidas para dichas conexiones.
•Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

9. POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN DE EMPLEADOS

COOUNISAN reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos empleados se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los empleados en sus cargos.

9.1.1. Normas relacionadas con la vinculación de empleados

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en COOUNISAN, antes de su vinculación definitiva.
•Gestión Humana debe certificar que los empleados de la compañía firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: SISTEMAS

•Informática debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de EMPRESA.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

•El personal provisto por terceras partes que realicen labores en o para COUNISAN, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
•El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información de la compañía.

9.2. POLÍTICA APLICABLE DURANTE LA VINCULACIÓN DE EMPLEADOS Y PERSONAL PROVISTO POR TERCEROS

COOUNISAN en su interés por proteger su información y los recursos de procesamiento de esta demostrará el compromiso de la Gerencia en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Compañía.

Todos los empleados de COOUNISAN deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Compañía.

9.2.1. Normas aplicables durante la vinculación de empleados y personal provisto por terceros

Normas dirigidas a: GERENCIA

•La Gerencia debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer la compañía.
•La Gerencia General debe promover la importancia de la seguridad de la información entre los empleados de COOUNISAN y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
•La Gerencia General debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente de la compañía, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Normas dirigidas a: SISTEMAS

•Informática debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
•Informática debe capacitar y entrenar a los empleados de COOUNISAN en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe aplicar el proceso disciplinario de la compañía cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.
•Gestión Humana debe convocar a los empleados a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Normas dirigidas a: TODOS LOS USUARIOS

•Los empleados y personal provisto por terceras partes que por sus funciones hagan uso de la información de COOUNISAN, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

9.3. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS EMPLEADOS Y PERSONAL PROVISTO POR TERCEROS

COOUNISAN asegurará que sus empleados y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

9.3.1. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los empleados y personal provisto por terceros

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los empleados de la compañía llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
•Gestión Humana debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a sistemas.

10. **POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN**

10.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

COOUNISAN como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.
La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones teléfonos, entre otros) propiedad de COOUNISAN, son activos de la compañía y se proporcionan a los empleados y terceros autorizados, para cumplir con los propósitos del negocio.
Toda la información sensible del COOUNISAN, así como los activos donde ésta se almacena y se procesa, deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte Gestión Humana.
Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

10.1.1. Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

•La Gerencia de COOUNISAN, deben actuar como propietaria de la información física y electrónica de la compañía, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

•Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de

la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
•Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
•Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la compañía se encuentran sujetos a auditorías por parte de Gestión Humana.

Normas dirigidas a: SISTEMAS

•Es la propietaria de los activos de información correspondientes a la plataforma tecnológica de COOUNISAN y, en consecuencia, debe asegurar su apropiada operación y administración.
•Es quien deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de COOUNISAN.
•Debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
•Es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los empleados y de hacer entrega de estas.
•Es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los empleados que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a: Gerencia

•La Gerencia, o quien ellos designen, deben autorizar a sus empleados el uso de los recursos tecnológicos, previamente preparados por sistemas.
•La Gerencia, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la compañía o son trasladados de área.

Normas dirigidas a: TODOS LOS USUARIOS

•Los recursos tecnológicos de COOUNISAN, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la compañía.
•Los recursos tecnológicos de COOUNISAN provistos a empleados y personal suministrado por terceras partes son proporcionados con el único fin de llevar a cabo las labores de la compañía; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

•Los empleados no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
•Los empleados no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de COOUNISAN.
•Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
•En el momento de desvinculación o cambio de labores, los empleados deben realizar la entrega de su puesto de trabajo al jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

10.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

COOUNISAN definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.

Toda la información de COOUNISAN debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por Gestión Humana.

Una vez clasificada la información, COOUNISAN proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los empleados de la compañía y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

10.2.1. Normas para la clasificación y manejo de la información

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe definir los niveles de clasificación de la información para COOUNISAN y, posteriormente generar la guía de clasificación de la Información.
•Gestión Humana debe socializar y divulgar la guía de clasificación de la Información a los empleados de la compañía.
•Gestión Humana debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

Normas dirigidas a: Sistemas

•Debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
•Debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
•Debe definir los métodos de cifrado de la información de la Compañía de acuerdo con el nivel de clasificación de los activos.

Normas dirigidas a: COORDINACIÓN DE ARCHIVO

•La Coordinación de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de esta, acogiéndose a procedimiento establecido para tal fin.
•La Coordinación de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.
•La Coordinación de Archivo debe administrar los documentos físicos de EMPRESA.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

•Los propietarios de los activos de información deben clasificar su información de acuerdo con las guías de clasificación de la Información establecida.
•Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la compañía.
•Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen y saquen copias: verificar las áreas adyacentes a impresoras, escáneres y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las

impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

•Tanto los empleados como el personal provisto por terceras partes deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

•La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

10.3. POLÍTICA PARA USO DE TOKENS DE SEGURIDAD

COOUNISAN proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los empleados hagan un uso responsable de estos.

10.3.1. Normas para uso de tokens de seguridad

Normas dirigidas a: ADMINISTRADORES DE LOS TOKENS DE SEGURIDAD

•Los Administradores de los tokens de seguridad deben procesar las solicitudes de dichos tokens según los requerimientos de cada compañía proveedora de éstos y adjuntar la documentación necesaria.

•Los Administradores de los tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.

•Los Administradores de los tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.

•Los Administradores de los tokens deben entregar a los empleados designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta para custodia de estos.

•Los Administradores de los tokens deben dar avisos a las compañías emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.

•Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la compañía emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: USUARIOS DE TOKENS DE SEGURIDAD

•Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.
•Los usuarios deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con COOUNISAN se dé por terminado o haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la compañía.
•Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
•El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
•Los usuarios deben notificar al proveedor de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las compañías emisoras de dichos tokens.
•Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.
•Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como empleados de COOUNISAN. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
•Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.

•Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
•Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
•Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.
•Los usuarios no deben usar los tokens fuera de las instalaciones de EMPRESA para evitar pérdida o robo de estos.

10.4. POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de COOUNISAN será reglamentado por Informática, junto con Gestión Humana, considerando las labores realizadas por los empleados y su necesidad de uso.

10.4.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: SISTEMAS Y GESTIÓN HUMANA

•Sistemas y Gestión Humana deben establecer las condiciones de uso de dispositivos de almacenamiento en la plataforma tecnológica de COOUNISAN.

Normas dirigidas a: SISTEMAS

•Debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la compañía, de acuerdo con los lineamientos y condiciones establecidas.
•Debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la compañía, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: TODOS LOS USUARIOS

•Los empleados y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por informática.
•Los empleados de COOUNISAN y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por Informática.
•Los empleados y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento asignados.
•Los empleados y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de COOUNISAN.

11. POLÍTICAS DE CONTROL DE ACCESO

11.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

Informática de COOUNISAN, como responsables de las redes de datos y los recursos de red de la compañía, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

11.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: SISTEMAS

•Debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de COOUNISAN.
•Debe asegurar que las redes inalámbricas de la compañía cuenten con métodos de autenticación que evite accesos no autorizados.
•Debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de COOUNISAN, así como velar por la aceptación de las responsabilidades de dicho terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

Normas dirigidas a: Gestión Humana

•Gestión Humana debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red del COOUNISAN.
•Gestión Humana debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: TODOS LOS USUARIOS

•Los empleados y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de COOUNISAN, deben contar con el Acuerdo de Confidencialidad firmado previamente.
•Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la compañía deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

11.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

COOUNISAN establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la compañía. Así mismo, velará porque los empleados y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque

la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

11.2.1. Normas de administración de acceso de usuarios

Normas dirigidas a: SISTEMAS

•Debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la compañía, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
•Previa solicitud de Gerencia, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
•Debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de COOUNISAN; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
•Debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los empleados se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
•Debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Normas dirigidas a: GESTIÓN HUMANA

•Debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la compañía.

11.3. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de COOUNISAN realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

11.3.1. Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de COOUNISAN deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

•Los empleados no deben compartir sus cuentas de usuario y contraseñas con otros empleados o con personal provisto por terceras partes.
•Los empleados y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la compañía deben acogerse a lineamientos para la configuración de contraseñas implantados por la compañía.

11.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

SISTEMAS de COOUNISAN velará porque los recursos de la plataforma tecnológica y los servicios de red de la compañía sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichas plataforma y servicios.

11.4.1. Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: SISTEMAS

•Debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos empleados designados para dichas funciones.
•Informática debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
•Informática debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.
•Informática debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
•Informática debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
•Informática debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

•Los administradores de los recursos tecnológicos y servicios de red, empleados de Informática, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de EMPRESA.
•Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
•Informática debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

11.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La Gerencia General como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

Informática, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

11.5.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

•Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
•Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: INFORMÁTICA

•Informática debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de COOUNISAN.

12. POLÍTICAS DE CRIPTOGRAFÍA

12.1. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

COOUNISAN velará porque la información de la Cooperativa, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

12.1.1. Normas de controles criptográficos

Normas dirigidas a: INFORMÁTICA

•Informática debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
•Informática debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
•Informática debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
•Informática, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

13. POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

13.1. POLÍTICA DE ÁREAS SEGURAS

COOUNISAN proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

13.1.1. Normas de áreas seguras

Normas dirigidas a: INFORMÁTICA

•Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por empleados de Informática autorizados; no obstante, los visitantes siempre

deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

•Informática debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un empleado autorizado.

•Informática debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

•Informática debe velar porque los recursos de la plataforma tecnológica de COOUNISAN ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

•Informática debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

•Informática debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: TODOS LOS USUARIOS

•Los ingresos y egresos de personal a las instalaciones de COOUNISAN deben ser registrados; por consiguiente, los empleados y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

•Los empleados deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de COOUNISAN; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

•Aquellos empleados o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

•Los empleados de COOUNISAN y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

13.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

COOUNISAN para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la compañía que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

13.2.1. Normas de seguridad para los equipos institucionales

Normas dirigidas a: INFORMÁTICA

•Informática debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de COOUNISAN.
•Informática debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la compañía.
•Informática debe generar estándares de configuración segura para los equipos de cómputo de los empleados de la Cooperativa y configurar dichos equipos acogiendo los estándares generados.
•Informática debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la compañía y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
•Informática debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los empleados de la compañía, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: TODOS LOS USUARIOS

•Informática es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Cooperativa.

•Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los empleados y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione Informática.
•Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de COOUNISAN el usuario responsable debe informar al área de Sistemas en donde se atenderá o escalará al interior de Informática, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

•La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la compañía, solo puede ser realizado por los empleados de Informática, o personal de terceras partes autorizado por dicha dirección.
•Los empleados de la Cooperativa y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
•Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
•En caso de pérdida o robo de un equipo de cómputo de COOUNISAN, se debe informar de forma inmediata al jefe inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
•Los empleados de la Cooperativa y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

14. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

14.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

Informática, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de COOUNISAN, asignará funciones específicas a sus empleados, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

Informática proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Cooperativa, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

14.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a: INFORMÁTICA

•Informática debe efectuar, a través de sus empleados, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la compañía.
•Informática debe proporcionar a sus empleados manuales de configuración y operación de los sistemas operativos, firmare, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de COOUNISAN.
•Informática, a través de sus empleados, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

14.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

COOUNISAN proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus empleados y personal provisto por terceras partes frente a los ataques de software malicioso.

14.2.1. Normas de protección frente a software malicioso

Normas dirigidas a: INFORMÁTICA

•Informática debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de COOUNISAN y los servicios que se ejecutan en la misma.
•Informática debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
•Informática debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
•Informática, a través de sus empleados, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

•Informática, a través de sus empleados, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por Informática; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
•Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
•Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
•Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de Sistemas, para que a través de ella, Informática tome las medidas de control correspondientes.

14.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

COOUNISAN certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de Informática, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la compañía velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Los respaldos de la información se realizarán cada semana en medio de almacenamiento externo y a su vez se realizará una retención mensual durante todo el año presente y al momento del cambio de año se retendrá la última copia del año anterior.

14.3.1. Normas de copias de respaldo de la información

Normas dirigidas a: INFORMÁTICA

•Informática, a través de sus empleados, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
•Informática debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
•Informática, a través de sus empleados, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
•Informática debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
•Informática debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la Cooperativa.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

•Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con Informática, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

•Es responsabilidad de los usuarios de la plataforma tecnológica de COOUNISAN identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

14.4. POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

COOUNISAN realizará monitoreo permanente del uso que dan los empleados y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la Cooperativa. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

14.4.1. Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: INFORMÁTICA

•Informática debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de COOUNISAN.
•Informática, a través de sus empleados, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
•Informática debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de COOUNISAN. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
•Informática debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

14.5. POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

COOUNISAN, a través de Informática, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Normas de control al software operativo

Normas dirigidas a: INFORMÁTICA

•Informática debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Cooperativa.
•Informática debe asegurarse que el software operativo instalado en la plataforma tecnológica de COOUNISAN cuenta con soporte de los proveedores.

•Informática debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
•Informática debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
•Informática debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Cooperativa.

14.6. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

COOUNISAN, a través de Informática revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

14.6.1. Normas para la gestión de vulnerabilidades

Normas dirigidas a: INFORMÁTICA

•Informática debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica, con el fin de prevenir la exposición al riesgo de estos.
•Informática, a través de sus empleados, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

15. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

15.1. POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

COOUNISAN establecerá, a través de Informática, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad, la disponibilidad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Cooperativa.

15.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: INFORMÁTICA

•Informática debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de COOUNISAN.
•Informática debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
•Informática debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para Cooperativa.
•Informática debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
•Informática debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la compañía, acogiendo buenas prácticas de configuración segura.
•Informática, a través de sus empleados, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la compañía en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
•Informática debe instalar protección entre las redes internas de COOUNISAN y cualquier red externa, que este fuera de la capacidad de control y administración de la compañía.
•Informática debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de COOUNISAN.

15.2. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

COOUNISAN, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre empleados y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

15.2.1. Normas de uso del correo electrónico

Normas dirigidas a: INFORMÁTICA

•Informática debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
•Informática debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
•Informática debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
•Informática, con el apoyo de Gestión Humana, debe generar campañas para concientizar tanto a los empleados internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

•La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la compañía o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
•Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de COOUNISAN. El correo institucional no debe ser utilizado para actividades personales.
•Los mensajes y la información contenida en los buzones de correo son propiedad de COOUNISAN y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
•Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los empleados de la compañía y el personal provisto por terceras partes.
•No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
•Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por COOUNISAN y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

15.3. POLÍTICA DE USO ADECUADO DE INTERNET

COOUNISAN consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la compañía.

15.3.1. Normas de uso adecuado de internet

Normas dirigidas a: INFORMÁTICA

•Informática debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
•Informática debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
•Informática debe monitorear continuamente el canal o canales del servicio de Internet.

•Informática debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios del servicio de Internet de COOUNISAN deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
•Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
•No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, Hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
•Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de COOUNISAN.
•No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o

confidencialidad de la infraestructura tecnológica (Hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo e Informática, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
•No está permitido el intercambio no autorizado de información propiedad de COOUNISAN, de sus cliente, empleados, terceros y con personas agenas a la Cooperativa.

16. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

16.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

COOUNISAN asegurará que el software adquirido, cumplirá con los requisitos de seguridad y calidad. Las áreas propietarias de sistemas de información incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad.

16.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN E INFORMÁTICA.

•Todos los sistemas de información deben tener un área propietaria dentro de la Cooperativa formalmente asignada.
•Las áreas propietarias de los sistemas de información, en acompañamiento con Informática deben establecer las especificaciones de adquisición de sistemas de información, considerando requerimientos de seguridad de la información.
•Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
•Informática debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
•seguros.

17. POLÍTICAS QUE RIGEN DE LA RELACIÓN CON TERCERAS PARTES

POLÍTICA DE INCLUSIÓN DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

COOUNISAN establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.
Los empleados responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

17.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: INFORMÁTICA Y JURÍDICA

•Informática y Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
•Informática y Jurídica deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: INFORMÁTICA

•Informática debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la compañía.

•Informática debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
•Informática debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de COOUNISAN.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

•Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de COOUNISAN a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

17.2. POLÍTICA DE GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

COOUNISAN propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

17.2.1. Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: INFORMÁTICA

•Informática debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la compañía.
•Informática debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: GESTIÓN HUMANA Y SUPERVISORES DE CONTRATOS CON TERCEROS

•Gestión Humana y los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

•Los Supervisores de contratos con terceros, con el apoyo de Gestión Humana, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

18. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

18.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

COOUNISAN promoverá entre los empleados y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
La Gerencia General o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante compañías externas.

18.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los activos de información deben informar a Gestión Humana, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
•Gestión Humana debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a Informática aquellos en los que se considere pertinente.
•Gestión Humana debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
•Gestión Humana debe, con el apoyo con Informática crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a: TODOS LOS USUARIOS

•Es responsabilidad de los empleados de COOUNISAN y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

•En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los empleados deben notificarlo a Gestión Humana para que se registre y se le dé el trámite necesario.

19. POLÍTICAS DE CUMPLIMIENTO

20.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS

LEGALES Y CONTRACTUALES

COOUNISAN velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

20.1.1. NORMAS DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

Normas dirigidas a: JURÍDICA

•Jurídica debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Cooperativa y relacionados con seguridad de la información.

Normas dirigidas a: INFORMÁTICA

•Informática debe certificar que todo el software que se ejecuta en la compañía esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
•Informática debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la compañía para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

•Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

20.2. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, COOUNISAN a través de Informática y Gestión Humana, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales COOUNISAN, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la compañía, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, COOUNISAN exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus empleados, estableciendo los controles necesarios para preservar aquella información que la compañía conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la compañía y no sea publicada, revelada o entregada a empleados o terceras partes sin autorización.

20.2.1. Normas de privacidad y protección de datos personales

Normas dirigidas a: ÁREAS QUE PROCESAN DATOS PERSONALES

•Las áreas que procesan datos personales empleados, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades del compañía.
•Las áreas que procesan datos personales empleados, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

•Las áreas que procesan datos personales empleados, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las compañías vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
•Las áreas que procesan datos personales empleados, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
•Las áreas que procesan datos personales proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: GESTIÓN HUMANA

•Gestión Humana debe establecer los controles para el tratamiento y protección de los datos personales de los empleados, proveedores y demás terceros de COOUNISAN de los cuales reciba y administre información.

Normas dirigidas a: INFORMÁTICA

•Informática debe implantar los controles necesarios para proteger la información personal de los empleados, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a: TODOS LOS USUARIOS

•Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la compañía o de sus empleados de cual tengan conocimiento en el ejercicio de sus funciones.
•Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

La presente política se firma en Santa Rosa de Osos a los cinco (05) días del mes de enero de 2022.